(Corresponding to US 2004/0006703 A1)

(22)

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-173215

(43)Date of publication of application : 20.06.2003

(51)Int.Cl. G06F 1/00
G06F 12/14
G09C 1/00
H04L 9/32

(21)Application number : 2002-145264

(22)Date of filing : 20.05.2002

(71)Applicant : SONY CORP

(72)Inventor : KITANI SATOSHI
MORIKAZU MUNETOSHI

(30)Priority

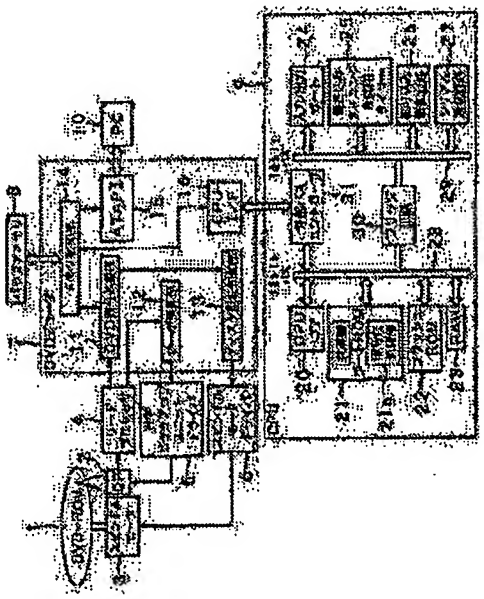
Priority number : 2001294506 Priority date : 26.09.2001 Priority country : JP

(54) INFORMATION PROCESSOR, PROGRAM LOADING METHOD, RECORDING MEDIUM, PROGRAM UPDATING METHOD AND CIRCUIT ELEMENT

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent leakage of program data during a program update.

SOLUTION: A control part 9 is provided with a ciphered program data receiving part 31 receiving ciphered program data of a second program ciphered by a predetermined cipher key in response to a program update request requesting update of a first program, a deciphering part 21a deciphering the ciphered program data received by the ciphered program data receiving part 31 into the second program by using a predetermined decipher key, program writing parts 20 and 21 writing the second program deciphered from the ciphered program data by the deciphering part 21a into a storing part 22, and a fetch limiting part 31 limiting fetching of the second program deciphered by the deciphering part 21a and the second program written in the storing part 22 from an external device.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－173215
（P2003－173215A）
(43)公開日　平成15年６月20日(2003.6.20)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)
G06F	1/00		G06F	12/14	320B 5B017
	12/14	320	G09C	1/00	640D 5B076
G09C	1/00	640	G06F	9/06	660L 5J104
H04L	9/32		H04L	9/00	675A

審査請求　未請求　請求項の数81　ＯＬ　（全 33 頁）

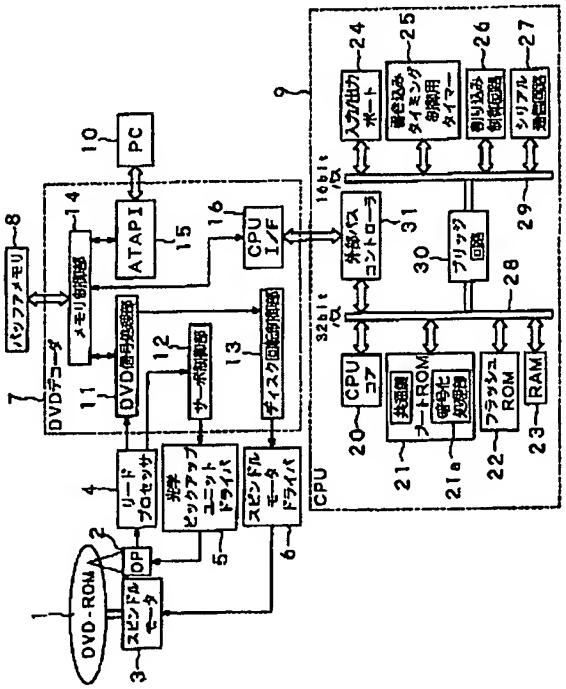
(21)出願番号　特願2002－145264(P2002－145264)
(22)出願日　平成14年５月20日(2002.5.20)
(31)優先権主張番号　特願2001－294506(P2001－294506)
(32)優先日　平成13年９月26日(2001.9.26)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　木谷　聡
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　盛一　宗利
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100067736
弁理士　小池　晃　（外２名）

最終頁に続く

(54)【発明の名称】　情報処理装置、プログラムロード方法、記録媒体、プログラム更新方法及び回路素子

(57)【要約】
【課題】　プログラム更新時のプログラムデータの漏洩を防止する。
【解決手段】　制御部９は、第１のプログラムの更新を要求するプログラム更新要求に応じて、第２のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信部３１と、暗号化プログラムデータ受信部３１で受信した暗号化プログラムデータを所定の復号鍵を用いて第２のプログラムに復号する復号部２１ａと、復号部２１ａで暗号化プログラムデータから復号された第２のプログラムを、記憶部２２に書き込むプログラム書き込み部２０，２１と、復号部２１ａで復号された第２のプログラム及び記憶部２２に書き込まれた第２のプログラムの外部装置からの取り出しを制限する取り出し制限部３１とを備えることで実現する。



1

【特許請求の範囲】

【請求項１】　所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信手段と、

上記暗号化プログラムデータ受信手段で受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記所定のプログラムに復号する復号手段と、

上記復号手段で上記暗号化プログラムデータから復号された上記所定のプログラムを記憶する記憶手段と、

上記記憶手段に記憶された上記所定のプログラムを読み出すプログラム読み出し手段と、

上記読み出し手段によって読み出された上記所定のプログラムに基づいて当該情報処理装置の所定の動作を制御する制御手段とを備えることを特徴とする情報処理装置。

【請求項２】　上記暗号化プログラムデータ受信手段は、外部装置から送信される暗号化プログラムデータを受信することを特徴とする請求１記載の情報処理装置。

【請求項３】　上記所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータが記録された記録媒体を再生する再生手段を備え、

上記暗号化プログラムデータ受信手段は、上記再生手段で再生された上記暗号化プログラムデータを受信することを特徴とする請求項１記載の情報処理装置。

【請求項４】　上記暗号化プログラムデータが記憶された暗号化プログラムデータ記憶手段を備え、

上記暗号化プログラムデータ記憶手段に記憶されている上記暗号化プログラムデータを読み出す暗号化プログラムデータ読み出し手段と、

上記暗号化プログラムデータ受信手段は、上記暗号化プログラムデータ読み出し手段によって読み出された上記暗号化プログラムデータを受信することを特徴とする請求項１記載の情報処理装置。

【請求項５】　上記暗号化プログラムデータ受信手段で受信される暗号化プログラムデータは、上記所定のプログラムのプログラムデータから所定の演算によって算出された第１の検証データと、上記所定の演算をするプログラムである検証プログラムとが上記所定の暗号化鍵で暗号化された暗号化検証データと、暗号化検証プログラムとを含むことを特徴とする請求項１記載の情報処理装置。

【請求項６】　上記復号手段は、上記暗号化プログラムデータを復号する際、上記暗号化検証データと、上記暗号化検証プログラムとを上記所定の復号鍵を用いて上記第１の検証データと、上記検証プログラムに復号し、

上記記憶手段は上記復号手段で復号された上記第１の検証データと、上記検証プログラムとを記憶し、

上記制御手段は、上記所定のプログラムを実行する前に、上記検証プログラムに基づいて、上記記憶手段に記憶された上記所定のプログラムのプログラムデータから

2

第２の検証データを算出し、算出された上記第２の検証データと、上記記憶手段に記憶されている上記第１の検証データとを比較し、

上記読み出し手段は、上記制御手段によって比較された上記第１の検証データと、上記第２の検証データとが一致したことに応じて、上記記憶手段に記憶されている上記所定のプログラムを読み出すことを特徴とする請求項５記載の情報処理装置。

【請求項７】　情報処理装置に所定のプログラムをロードするためのプログラムロード方法であって、

上記所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信ステップと、

上記暗号化プログラムデータ受信ステップで受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記所定のプログラムに復号する復号ステップと、

上記復号ステップで上記暗号化プログラムデータから復号された上記所定のプログラムを記憶手段に記憶する記憶ステップと、

上記記憶手段に記憶された上記所定のプログラムを読み出すプログラム読み出しステップと、

上記読み出しステップによって読み出された上記所定のプログラムに基づいて当該情報処理装置の所定の動作を制御する制御ステップとを備えることを特徴とするプログラムロード方法。

【請求項８】　上記暗号化プログラムデータ受信ステップは、外部装置から送信される暗号化プログラムデータを受信することを特徴とする請求７記載のプログラムロード方法。

【請求項９】　上記所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータが記録された記録媒体を再生する再生ステップを備え、

上記暗号化プログラムデータ受信ステップは、上記再生ステップで再生された上記暗号化プログラムデータを受信することを特徴とする請求項７記載のプログラムロード方法。

【請求項１０】　上記暗号化プログラムデータが記憶されている当該情報処理装置に備えられた暗号化プログラムデータ記憶手段から上記暗号化プログラムデータを読み出す暗号化プログラムデータ読み出しステップを備え、

上記暗号化プログラムデータ受信ステップは、上記暗号化プログラム読み出しステップによって読み出された上記暗号化プログラムデータを受信することを特徴とする請求項７記載のプログラムロード方法。

【請求項１１】　上記暗号化プログラムデータ受信ステップは、上記所定のプログラムのプログラムデータから所定の演算によって算出された第１の検証データと、上記所定の演算をするプログラムである検証プログラムとが上記所定の暗号化鍵で暗号化された暗号化検証データ

と、暗号化検証プログラムとを含んだ上記暗号化プログラムデータを受信することを特徴とする請求項７記載のプログラムロード方法。

【請求項１２】　上記復号ステップは、上記暗号化プログラムデータを復号する際、上記暗号化検証データと、上記暗号化検証プログラムとを上記所定の復号鍵を用いて上記第１の検証データと、上記検証プログラムに復号し、

上記記憶ステップは、上記記憶手段に上記復号ステップで復号された上記第１の検証データと、上記検証プログラムとを記憶し、

上記制御ステップで、上記所定のプログラムを実行する前に、上記検証プログラムに基づいて、上記記憶手段に記憶された上記所定のプログラムのプログラムデータから第２の検証データを算出する検証データ算出ステップと、

上記検証データ算出ステップで算出された上記第２の検証データと、上記記憶手段に記憶されている上記第１の検証データとを比較する検証データ比較ステップとを備え、

上記読み出しステップは、上記検証データ比較ステップによって比較された上記第１の検証データと、上記第２の検証データとが一致したことに応じて、上記記憶手段に記憶されている上記所定のプログラムを読み出すことを特徴とする請求項１１記載のプログラムロード方法。

【請求項１３】　情報処理装置に所定のプログラムをロードするためのプログラムを記録した記録媒体であって、

上記所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信ステップと、

上記暗号化プログラムデータ受信ステップで受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記所定のプログラムに復号する復号ステップと、上記復号ステップで上記暗号化プログラムデータから復号された上記所定のプログラムを記憶手段に記憶する記憶ステップと、

上記記憶手段に記憶された上記所定のプログラムを読み出すプログラム読み出しステップと、

上記読み出しステップによって読み出された上記所定のプログラムに基づいて当該情報処理装置の所定の動作を制御する制御ステップとを備えることを特徴とするプログラムを記録した記録媒体。

【請求項１４】　上記暗号化プログラムデータ受信ステップは、外部装置から送信される暗号化プログラムデータを受信することを特徴とするプログラムを記録した請求１３記載の記録媒体。

【請求項１５】　上記所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータが記録された記録媒体を再生する再生ステップを備え、

上記暗号化プログラムデータ受信ステップは、上記再生ステップで再生された上記暗号化プログラムデータを受信することを特徴とするプログラムを記録した請求項１３記載の記録媒体。

【請求項１６】　上記暗号化プログラムデータが記憶されている当該情報処理装置に備えられた暗号化プログラムデータ記憶手段から上記暗号化プログラムデータを読み出す暗号化プログラムデータ読み出しステップを備え、

上記暗号化プログラムデータ受信ステップは、上記暗号化プログラム読み出しステップによって読み出された上記暗号化プログラムデータを受信することを特徴とするプログラムを記録した請求項１３記載の記録媒体。

【請求項１７】　上記暗号化プログラムデータ受信ステップは、上記所定のプログラムのプログラムデータから所定の演算によって算出された第１の検証データと、上記所定の演算をするプログラムである検証プログラムとが上記所定の暗号化鍵で暗号化された暗号化検証データと、暗号化検証プログラムとを含んだ上記暗号化プログラムデータを受信することを特徴とするプログラムを記録した請求項１３記載の記録媒体。

【請求項１８】　上記復号ステップは、上記暗号化プログラムデータを復号する際、上記暗号化検証データと、上記暗号化検証プログラムとを上記所定の復号鍵を用いて上記第１の検証データと、上記検証プログラムに復号し、

上記記憶ステップは、上記記憶手段に上記復号ステップで復号された上記第１の検証データと、上記検証プログラムとを記憶し、

上記制御ステップで、上記所定のプログラムを実行する前に、上記検証プログラムに基づいて、上記記憶手段に記憶された上記所定のプログラムのプログラムデータから第２の検証データを算出する検証データ算出ステップと、

上記検証データ算出ステップで算出された上記第２の検証データと、上記記憶手段に記憶されている上記第１の検証データとを比較する検証データ比較ステップとを備え、

上記読み出しステップは、上記検証データ比較ステップによって比較された上記第１の検証データと、上記第２の検証データとが一致したことに応じて、上記記憶手段に記憶されている上記所定のプログラムを読み出すことを特徴とするプログラムを記録した請求項１７記載の記録媒体。

【請求項１９】　第１のプログラムが記憶された記憶手段と、上記記憶手段に記憶されている上記第１のプログラムを読み出し、読み出した上記第１のプログラムに基づいて当該情報処理装置の所定の動作を制御する制御手段とを有する制御部を備えた情報処理装置であって、

上記制御部は、

上記第１のプログラムの更新を要求するプログラム更新要求に応じて、第２のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信手段と、

上記暗号化プログラムデータ受信手段で受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記第２のプログラムに復号する復号手段と、

上記復号手段で上記暗号化プログラムデータから復号された第２のプログラムを、上記記憶手段に書き込むプログラム書き込み手段と、

上記復号手段で復号された第２のプログラム及び上記記憶手段に書き込まれた第２のプログラムの外部装置からの取り出しを制限する取り出し制限手段とを備えることを特徴とする情報処理装置。

【請求項２０】　上記暗号化プログラムデータ受信手段は、外部装置から送信される暗号化プログラムデータを受信することを特徴とする請求項１９記載の情報処理装置。

【請求項２１】　上記第２のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータが記録された記録媒体を再生する再生手段を備え、

上記制御手段は、上記プログラム更新要求に応じて、上記記録媒体を再生させるよう上記再生手段を制御し、

上記暗号化プログラムデータ受信手段は、上記再生手段で再生された上記暗号化プログラムデータを受信することを特徴とする請求項１９記載の情報処理装置。

【請求項２２】　上記暗号化プログラムデータ受信手段で受信される暗号化プログラムデータは、上記第２のプログラムのプログラムデータから所定の演算によって算出された第１の検証データと、上記所定の演算をするプログラムである検証プログラムとが上記所定の暗号化鍵で暗号化された暗号化検証データと、暗号化検証プログラムとを含むことを特徴とする請求項１９記載の情報処理装置。

【請求項２３】　上記復号手段は、上記暗号化プログラムデータを復号する際、上記暗号化検証データと、上記暗号化検証プログラムとを上記所定の復号鍵を用いて上記第１の検証データと、上記検証プログラムに復号し、

上記プログラム書き込み手段は、上記復号手段で復号された上記第１の検証データと、上記検証プログラムとを上記記憶手段に書き込み、

上記制御手段は、上記第２のプログラムを実行する前に、上記検証プログラムに基づいて、上記記憶手段に記憶された上記第２のプログラムのプログラムデータから第２の検証データを算出し、算出された上記第２の検証データと、上記記憶手段に記憶されている上記第１の検証データとを比較し、比較した上記第１の検証データと、上記第２の検証データとが一致したことに応じて、上記記憶手段に記憶されている上記第２のプログラムを読み出すことを特徴とする請求項２２記載の情報処理装置。

【請求項２４】　第１のプログラムが記憶された記憶手段と、上記記憶手段に記憶されている上記第１のプログラムを読み出し、読み出した上記第１のプログラムに基づいて当該情報処理装置の所定の動作を制御する制御手段とを有する制御部を備えた情報処理装置のプログラム更新方法であって、

上記第１のプログラムの更新を要求するプログラム更新要求に応じて、第２のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信ステップと、

上記受信した暗号化プログラムデータを所定の復号鍵を用いて上記第２のプログラムに復号する復号ステップと、

上記復号された第２のプログラムの外部装置からの取り出しを制限する取り出し制限ステップと、

上記暗号化プログラムデータから復号された第２のプログラムを、上記記憶手段に書き込むプログラム書き込みステップとを備えることを特徴とするプログラム更新方法。

【請求項２５】　上記暗号化プログラムデータ受信ステップでは、外部装置から送信される暗号化プログラムデータを受信することを特徴とする請求項２４記載のプログラム更新方法。

【請求項２６】　上記第２のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータが記録された記録媒体を再生する再生ステップを備え、

上記再生ステップは、上記プログラム更新要求を受信したことに応じて上記記録媒体を再生させ、

上記暗号化プログラムデータ受信ステップは、上記再生された暗号化プログラムデータを受信することを特徴とする請求項２４記載のプログラム更新方法。

【請求項２７】　上記暗号化プログラムデータ受信ステップは、上記第２のプログラムのプログラムデータから所定の演算によって算出された第１の検証データと、上記所定の演算をするプログラムである検証プログラムとが上記所定の暗号化鍵で暗号化された暗号化検証データと、暗号化検証プログラムとを含んだ上記暗号化プログラムデータを受信することを特徴とする請求項２４記載のプログラム更新方法。

【請求項２８】　上記復号ステップは、上記暗号化プログラムデータを復号する際、上記暗号化検証データと、上記暗号化検証プログラムとを上記所定の復号鍵を用いて上記第１の検証データと、上記検証プログラムに復号し、

上記プログラム書き込みステップは、上記復号ステップで復号された上記第１の検証データと、上記検証プログラムとを上記記憶手段に書き込み、

上記制御手段で上記第２のプログラムを実行する前に、上記検証プログラムに基づいて、上記記憶手段に記憶さ

れた上記第２のプログラムのプログラムデータから第２の検証データを算出する検証データ算出ステップと、
上記検証データ算出ステップで算出された上記第２の検証データと、上記記憶手段に記憶されている上記第１の検証データとを比較する検証データ比較ステップと、
上記検証データ比較ステップによって比較された上記第１の検証データと、上記第２の検証データとが一致したことに応じて、上記記憶手段に記憶されている上記第２のプログラムを読み出すプログラム読み出しステップとを備えることを特徴とする請求項２７記載のプログラム更新方法。

【請求項２９】　第１のプログラムが記憶された記憶手段と、上記記憶手段に記憶されている上記第１のプログラムを読み出し、読み出した上記第１のプログラムに基づいて所定の動作を制御する制御手段とを有する制御部を備えた情報処理装置の上記第１のプログラムを更新するためのプログラムを記録した記録媒体であって、
上記第１のプログラムの更新を要求するプログラム更新要求に応じて、第２のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信ステップと、
上記受信した暗号化プログラムデータを所定の復号鍵を用いて上記第２のプログラムに復号する復号ステップと、
上記復号された第２のプログラムの外部装置からの取り出しを制限する取り出し制限ステップと、
上記暗号化プログラムデータから復号された第２のプログラムを上記記憶手段に書き込むプログラム書き込みステップとを備えることを特徴とするプログラムを記録した記録媒体。

【請求項３０】　上記暗号化プログラムデータ受信ステップでは、外部装置から送信される暗号化プログラムデータを受信することを特徴とするプログラムを記録した請求項２９記載の記録媒体。

【請求項３１】　上記第２のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータが記録された当該記録媒体を再生する再生ステップを備え、
上記再生ステップは、上記プログラム更新要求を受信したことに応じて当該記録媒体に記録されている上記暗号化プログラムデータを再生させ、
上記暗号化プログラムデータ受信ステップは、上記再生された上記暗号化プログラムデータを受信することを特徴とするプログラムを記録した請求項２９記載の記録媒体。

【請求項３２】　上記暗号化プログラムデータ受信ステップは、上記第２のプログラムのプログラムデータから所定の演算によって算出された第１の検証データと、上記所定の演算をするプログラムである検証プログラムとが上記所定の暗号化鍵で暗号化された暗号化検証データと、暗号化検証プログラムとを含んだ上記暗号化プログラムデータを受信することを特徴とするプログラムを記録した請求項２９記載の記録媒体。

【請求項３３】　上記復号ステップは、上記暗号化プログラムデータを復号する際、上記暗号化検証データと、上記暗号化検証プログラムとを上記所定の復号鍵を用いて上記第１の検証データと、上記検証プログラムに復号し、
上記プログラム書き込みステップは、上記復号ステップで復号された上記第１の検証データと、上記検証プログラムとを上記記憶手段に書き込み、
上記制御手段で上記所定のプログラムを実行する前に、上記検証プログラムに基づいて、上記記憶手段に記憶された上記所定のプログラムのプログラムデータから第２の検証データを算出する検証データ算出ステップと、
算出された上記第２の検証データと、上記記憶手段に記憶されている上記第１の検証データとを比較する検証データ比較ステップと、
上記検証データ比較ステップによって比較された上記第１の検証データと、上記第２の検証データとが一致したことに応じて、上記記憶手段に記憶されている上記第２のプログラムを読み出すプログラム読み出しステップとを備えることを特徴とするプログラムを記録した請求項３２記載の記録媒体。

【請求項３４】　第１のプログラムが記憶された記憶手段と、上記記憶手段に記憶されている上記第１のプログラムを読み出し、読み出した上記第１のプログラムに基づいて情報処理装置の所定の動作を制御する制御手段とを集積化した回路素子であって、
上記第１のプログラムの更新を要求するプログラム更新要求に応じて、第２のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信手段と、
上記暗号化プログラムデータ受信手段で受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記第２のプログラムに復号する復号手段と、
上記復号手段で上記暗号化プログラムデータから復号された第２のプログラムを、上記記憶手段に書き込むプログラム書き込み手段と、
上記復号手段で復号された第２のプログラム及び上記記憶手段に書き込まれた第２のプログラムの外部装置からの取り出しを制限する取り出し制限手段とを集積化してなることを特徴とする回路素子。

【請求項３５】　上記暗号化プログラムデータ受信手段は、外部装置から送信される暗号化プログラムデータを受信することを特徴とする請求項３４記載の回路素子。

【請求項３６】　上記第２のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータが記録された記録媒体を再生する再生手段を備えた情報処理装置に備えられ、
上記制御手段は、上記プログラム更新要求に応じて、上

記記録媒体を再生させるよう上記再生手段を制御し、
上記暗号化プログラムデータ受信手段は、上記情報処理装置の再生手段で再生された上記暗号化プログラムデータを受信することを特徴とする請求項３４記載の回路素子。

【請求項３７】　上記暗号化プログラムデータ受信手段で受信される暗号化プログラムデータは、上記第２のプログラムのプログラムデータから所定の演算によって算出された第１の検証データと、上記所定の演算をするプログラムである検証プログラムとが上記所定の暗号化鍵で暗号化された暗号化検証データと、暗号化検証プログラムとを含むことを特徴とする請求項３４記載の回路素子。

【請求項３８】　上記復号手段は、上記暗号化プログラムデータを復号する際、上記暗号化検証データと、上記暗号化検証プログラムとを上記所定の復号鍵を用いて上記第１の検証データと、上記検証プログラムに復号し、
上記プログラム書き込み手段は、上記復号手段で復号された上記第１の検証データと、上記検証プログラムとを上記記憶手段に書き込み、
上記制御手段は、上記第２のプログラムを実行する前に、上記検証プログラムに基づいて、上記記憶手段に記憶された上記第２のプログラムのプログラムデータから第２の検証データを算出し、算出された上記第２の検証データと、上記記憶手段に記憶されている上記第１の検証データとを比較し、比較した上記第１の検証データと、上記第２の検証データとが一致したことに応じて、上記記憶手段に記憶されている上記第２のプログラムを読み出すことを特徴とする請求項３７記載の回路素子。

【請求項３９】　第１のプログラムが記憶された記憶手段と、上記記憶手段に記憶されている上記第１のプログラムを読み出し、読み出した上記第１のプログラムに基づいて当該情報処理装置の所定の動作を制御する制御手段とを有する制御部を備えた情報処理装置であって、
上記第１のプログラムの更新を要求するプログラム更新要求に応じて、第２のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信手段と、
上記暗号化プログラムデータ受信手段で受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記第２のプログラムに復号する復号手段と、
上記復号手段で上記暗号化プログラムデータから復号された上記第２のプログラムを上記制御部に送信するプログラム送信手段とを備え、
上記制御部は、上記送信手段によって送信された上記第２のプログラムを受信するプログラム受信手段と、
上記プログラム受信手段で受信した上記第２のプログラムを上記記憶手段に書き込むプログラム書き込み手段とを有することを特徴とする情報処理装置。

【請求項４０】　上記暗号化プログラムデータ受信手段は、外部装置から送信される暗号化プログラムデータを受信することを特徴とする請求項３９記載の情報処理装置。

【請求項４１】　上記第２のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータが記録された記録媒体を再生する再生手段を備え、
上記制御手段は、上記プログラム更新要求に応じて、上記記録媒体を再生させるよう上記再生手段を制御し、
上記暗号化プログラムデータ受信手段は、上記再生手段で再生された上記暗号化プログラムデータを受信することを特徴とする請求項３９記載の情報処理装置。

【請求項４２】　上記プログラム送信手段と上記プログラム受信手段とを接続する配線を多層基板の内層に施すことを特徴とする請求項３９記載の情報処理装置。

【請求項４３】　上記制御部は、ボールグリッドアレイであることを特徴とする請求項３９記載の情報処理装置。

【請求項４４】　上記暗号化プログラムデータ受信手段で受信される暗号化プログラムデータは、上記第２のプログラムのプログラムデータから所定の演算によって算出された第１の検証データと、上記所定の演算をするプログラムである検証プログラムとが上記所定の暗号化鍵で暗号化された暗号化検証データと、暗号化検証プログラムとを含むことを特徴とする請求項３９記載の情報処理装置。

【請求項４５】　上記復号手段は、上記暗号化プログラムデータを復号する際、上記暗号化検証データと、上記暗号化検証プログラムとを上記所定の復号鍵を用いて上記第１の検証データと、上記検証プログラムに復号し、
上記プログラム書き込み手段は、上記復号手段で復号された上記第１の検証データと、上記検証プログラムとを上記記憶手段に書き込み、
上記制御手段は、上記第２のプログラムを実行する前に、上記検証プログラムに基づいて、上記記憶手段に記憶された上記第２のプログラムのプログラムデータから第２の検証データを算出し、算出された上記第２の検証データと、上記記憶手段に記憶されている上記第１の検証データとを比較し、比較した上記第１の検証データと、上記第２の検証データとが一致したことに応じて、上記記憶手段に記憶されている上記第２のプログラムを読み出すことを特徴とする請求項４３記載の情報処理装置。

【請求項４６】　第１のプログラムが記憶された記憶手段と、上記記憶手段に記憶されている上記第１のプログラムを読み出し、読み出した上記第１のプログラムに基づいて当該情報処理装置の所定の動作を制御する制御手段とを有する制御部を備えた情報処理装置のプログラム更新方法であって、
上記第１のプログラムの更新を要求するプログラム更新要求に応じて、第２のプログラムを所定の暗号化鍵で暗

号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信ステップと、
上記暗号化プログラムデータ受信ステップで受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記第２のプログラムに復号する復号ステップと、
上記復号ステップで上記暗号化プログラムデータから復号された上記第２のプログラムを上記制御部に送信するプログラム送信ステップとを備え、
上記プログラム送信ステップによって上記制御部に送信された上記第２のプログラムを受信するプログラム受信ステップと、
上記プログラム受信ステップで受信した上記第２のプログラムを上記記憶手段に書き込むプログラム書き込みステップとを有することを特徴とするプログラム更新方法。

【請求項４７】　上記暗号化プログラムデータ受信ステップは、外部装置から送信される暗号化プログラムデータを受信することを特徴とする請求項４６記載のプログラム更新方法。

【請求項４８】　上記第２のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータが記録された記録媒体を再生する再生ステップを備え、
上記再生ステップは、上記プログラム更新要求を受信したことに応じて上記記録媒体を再生させ、
上記暗号化プログラムデータ受信ステップは、上記再生ステップで再生された上記暗号化プログラムデータを受信することを特徴とする請求項４６記載のプログラム更新方法。

【請求項４９】　上記暗号化プログラムデータ受信ステップは、上記第２のプログラムのプログラムデータから所定の演算によって算出された第１の検証データと、上記所定の演算をするプログラムである検証プログラムとが上記所定の暗号化鍵で暗号化された暗号化検証データと、暗号化検証プログラムとを含んだ上記暗号化プログラムデータを受信することを特徴とする請求項４６記載のプログラム更新方法。

【請求項５０】　上記復号ステップは、上記暗号化プログラムデータを復号する際、上記暗号化検証データと、上記暗号化検証プログラムとを上記所定の復号鍵を用いて上記第１の検証データと、上記検証プログラムに復号し、
上記プログラム書き込みステップは、上記復号ステップで復号された上記第１の検証データと、上記検証プログラムとを上記記憶手段に書き込み、
上記制御手段で上記第２のプログラムを実行する前に、上記検証プログラムに基づいて、上記記憶手段に記憶された上記第２のプログラムのプログラムデータから第２の検証データを算出する検証データ算出ステップと、
上記検証データ算出ステップで算出された上記第２の検証データと、上記記憶手段に記憶されている上記第１の検証データとを比較する検証データ比較ステップと、
上記検証データ比較ステップによって比較された上記第１の検証データと、上記第２の検証データとが一致したことに応じて、上記記憶手段に記憶されている上記第２のプログラムを読み出すプログラム読み出しステップとを備えることを特徴とする請求項４９記載のプログラム更新方法。

【請求項５１】　第１のプログラムが記憶された記憶手段と、上記記憶手段に記憶されている上記第１のプログラムを読み出し、読み出した上記第１のプログラムに基づいて当該情報処理装置の所定の動作を制御する制御手段とを有する制御部を備えた情報処理装置の上記第１のプログラムを更新するためのプログラムを記録した記録媒体であって、
上記第１のプログラムの更新を要求するプログラム更新要求に応じて、第２のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信ステップと、
上記暗号化プログラムデータ受信ステップで受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記第２のプログラムに復号する復号ステップと、
上記復号ステップで上記暗号化プログラムデータから復号された上記第２のプログラムを上記制御部に送信するプログラム送信ステップとを備え、
上記プログラム送信ステップによって上記制御部に送信された上記第２のプログラムを受信するプログラム受信ステップと、
上記プログラム受信ステップで受信した上記第２のプログラムを上記記憶手段に書き込むプログラム書き込みステップとを有することを特徴とするプログラムを記録した記録媒体。

【請求項５２】　上記暗号化プログラムデータ受信ステップは、外部装置から送信される暗号化プログラムデータを受信することを特徴とするプログラム記録した請求項５１記載の記録媒体。

【請求項５３】　上記第２のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータが記録された記録媒体を再生する再生ステップを備え、
上記再生ステップは、上記プログラム更新要求を受信したことに応じて上記記録媒体を再生させ、
上記暗号化プログラムデータ受信ステップは、上記再生ステップで再生された上記暗号化プログラムデータを受信することを特徴とするプログラムを記録した請求項５１記載の記録媒体。

【請求項５４】　上記暗号化プログラムデータ受信ステップは、上記第２のプログラムのプログラムデータから所定の演算によって算出された第１の検証データと、上記所定の演算をするプログラムである検証プログラムとが上記所定の暗号化鍵で暗号化された暗号化検証データと、暗号化検証プログラムとを含んだ上記暗号化プログ

ラムデータを受信することを特徴とするプログラムを記録した請求項５１記載の記録媒体。

【請求項５５】　上記復号ステップは、上記暗号化プログラムデータを復号する際、上記暗号化検証データと、上記暗号化検証プログラムとを上記所定の復号鍵を用いて上記第１の検証データと、上記検証プログラムに復号し、

上記プログラム書き込みステップは、上記復号ステップで復号された上記第１の検証データと、上記検証プログラムとを上記記憶手段に書き込み、

上記制御手段で上記第２のプログラムを実行する前に、上記検証プログラムに基づいて、上記記憶手段に記憶された上記第２のプログラムのプログラムデータから第２の検証データを算出する検証データ算出ステップと、

算出された上記第２の検証データと、上記記憶手段に記憶されている上記第１の検証データとを比較する検証データ比較ステップと、

上記検証データ比較ステップによって比較された上記第１の検証データと、上記第２の検証データとが一致したことに応じて、上記記憶手段に記憶されている上記第２のプログラムを読み出すプログラム読み出しステップと備えることを特徴とするプログラムを記録した請求項５４記載の記録媒体。

【請求項５６】　所定のデータ処理を行うデータ処理部を備えた情報処理装置であって、

上記データ処理部は、

所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信手段と、

上記暗号化プログラムデータ受信手段で受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記所定のプログラムに復号する復号手段と、

上記復号手段で上記暗号化プログラムデータから復号された上記所定のプログラムを記憶する記憶手段と、

上記記憶手段に記憶された上記所定のプログラムを読み出すプログラム読み出し手段と、

上記プログラム読み出し手段によって読み出された上記所定のプログラムに基づいて、当該データ処理部における所定のデータ処理動作を制御する第１の制御手段と、

上記復号手段で復号された上記所定のプログラム及び上記記憶手段に記憶された上記所定のプログラムの外部装置からの取り出しを制限する取り出し制限手段とを有することを特徴とする情報処理装置。

【請求項５７】　上記暗号化プログラムデータが記憶された暗号化プログラムデータ記憶手段を備え、

上記第１の制御手段は、上記暗号化プログラムデータ記憶手段に記憶されている上記暗号化プログラムデータを読み出し、

上記暗号化プログラムデータ受信手段は、上記第１の制御手段によって読み出された上記暗号化プログラムデータを受信することを特徴とする請求項５６記載の情報処理装置。

【請求項５８】　上記暗号化プログラムデータ記憶手段に記憶されている上記暗号化プログラムデータを読み出す第２の制御手段を備え、

上記暗号化プログラムデータ受信手段は、上記第２の制御手段によって読み出された上記暗号化プログラムデータを受信することを特徴とする請求項５６記載の情報処理装置。

【請求項５９】　上記暗号化プログラムデータ受信手段は、外部装置から送信される暗号化プログラムデータを受信することを特徴とする請求項５６記載の情報処理装置。

【請求項６０】　上記所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータが記録された記録媒体を再生する再生手段を備え、

上記第１の制御手段は、上記記録媒体を再生させるよう上記再生手段を制御し、

上記暗号化プログラムデータ受信手段は、上記再生手段で再生された上記暗号化プログラムデータを受信することを特徴とする請求項５６記載の情報処理装置。

【請求項６１】　上記暗号化プログラムデータ受信手段で受信される暗号化プログラムデータは、上記所定のプログラムのプログラムデータから所定の演算によって算出された第１の検証データと、上記所定の演算をするプログラムである検証プログラムとが上記所定の暗号化鍵で暗号化された暗号化検証データと、暗号化検証プログラムとを含むことを特徴とする請求項５６記載の情報処理装置。

【請求項６２】　上記復号手段は、上記暗号化プログラムデータを復号する際、上記暗号化検証データと、上記暗号化検証プログラムとを上記所定の復号鍵を用いて上記第１の検証データと、上記検証プログラムに復号し、

上記記憶手段は上記復号手段で復号された上記第１の検証データと、上記検証プログラムとを記憶し、

上記第１の制御手段は、上記所定のプログラムを実行する前に、上記検証プログラムに基づいて、上記記憶手段に記憶された上記所定のプログラムのプログラムデータから第２の検証データを算出し、算出された上記第２の検証データと、上記記憶手段に記憶されている上記第１の検証データとを比較し、

上記プログラム読み出し手段は、上記第１の制御手段によって比較された上記第１の検証データと、上記第２の検証データとが一致したことに応じて、上記記憶手段に記憶されている上記所定のプログラムを読み出すことを特徴とする請求項６１記載の情報処理装置。

【請求項６３】　所定のデータ処理を行うデータ処理部を備えた情報処理装置の上記データ処理部でのプログラムロード方法であって、

所定のプログラムを所定の暗号化鍵で暗号化した暗号化

プログラムデータを受信する暗号化プログラムデータ受信ステップと、
上記プログラムデータ受信ステップで受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記所定のプログラムに復号する復号ステップと、
上記復号された上記所定のプログラムの外部装置からの取り出しを制限する取り出し制限ステップと、
上記復号ステップで上記暗号化プログラムデータから復号された上記所定のプログラムを記憶手段に記憶させる記憶ステップと、
上記記憶手段に記憶された上記所定のプログラムを読み出すプログラム読み出しステップと、
上記プログラム読み出しステップによって読み出された上記所定のプログラムに基づいて、当該データ処理部における所定のデータ処理動作を制御する制御ステップと有することを特徴とするプログラムロード方法。

【請求項６４】 上記制御ステップは、上記暗号化プログラムデータが記憶されている当該情報処理装置に備えられた暗号化プログラムデータ記憶手段から上記暗号化プログラムデータを読み出し、
上記暗号化プログラムデータ受信ステップは、読み出された上記暗号化プログラムデータを受信することを特徴とする請求項６３記載のプログラムロード方法。

【請求項６５】 上記暗号化プログラムデータ受信ステップは、外部装置から送信される暗号化プログラムデータを受信することを特徴とする請求項６３記載のプログラムロード方法。

【請求項６６】 上記所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータが記録された記録媒体を再生する再生ステップを備え、
上記暗号化プログラムデータ受信ステップは、上記再生ステップで再生された上記暗号化プログラムデータを受信することを特徴とする請求項６３記載のプログラムロード方法。

【請求項６７】 上記暗号化プログラムデータ受信ステップは、上記所定のプログラムのプログラムデータから所定の演算によって算出された第１の検証データと、上記所定の演算をするプログラムである検証プログラムとが上記所定の暗号化鍵で暗号化された暗号化検証データと、暗号化検証プログラムとを含んだ上記暗号化プログラムデータを受信することを特徴とする請求項６３記載のプログラムロード方法。

【請求項６８】 上記復号ステップは、上記暗号化プログラムデータを復号する際、上記暗号化検証データと、上記暗号化検証プログラムとを上記所定の復号鍵を用いて上記第１の検証データと、上記検証プログラムに復号し、
上記記憶ステップは、上記記憶手段に上記復号ステップで復号された上記第１の検証データと、上記検証プログラムとを記憶し、

上記制御ステップで、上記所定のプログラムを実行する前に、上記検証プログラムに基づいて、上記記憶手段に記憶された上記所定のプログラムのプログラムデータから第２の検証データを算出する検証データ算出ステップと、
上記検証データ算出ステップによって算出された上記第２の検証データと、上記記憶手段に記憶されている上記第１の検証データとを比較する検証データ比較ステップとを備え、
上記プログラム読み出しステップは、上記検証データ比較ステップによって比較された上記第１の検証データと、上記第２の検証データとが一致したことに応じて、上記記憶手段に記憶されている上記所定のプログラムを読み出すことを特徴とする請求項６７記載のプログラムロード方法。

【請求項６９】 所定のデータ処理を行うデータ処理部を備えた情報処理装置の上記データ処理部で所定のプログラムをロードするためのプログラムを記録した記録媒体であって、
上記所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信ステップと、
上記プログラムデータ受信ステップで受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記所定のプログラムに復号する復号ステップと、
上記復号された上記所定のプログラムの外部装置からの取り出しを制限する取り出し制限ステップと、
上記復号ステップで上記暗号化プログラムデータから復号された上記所定のプログラムを記憶手段に記憶する記憶ステップと、
上記記憶手段に記憶された上記所定のプログラムを読み出すプログラム読み出しステップと、
上記プログラム読み出しステップによって読み出された上記所定のプログラムに基づいて、上記データ処理部における所定のデータ処理動作を制御する制御ステップと有することを特徴とするプログラムが記録された記録媒体。

【請求項７０】 上記制御ステップは、上記暗号化プログラムデータが記憶されている当該情報処理装置に備えられた暗号化プログラムデータ記憶手段に記憶されている上記暗号化プログラムデータを読み出し、
上記暗号化プログラムデータ受信ステップは、上記制御ステップによって読み出された上記暗号化プログラムデータを受信することを特徴とするプログラムが記録された請求項６９記載の記録媒体。

【請求項７１】 上記暗号化プログラムデータ受信ステップは、外部装置から送信される暗号化プログラムデータを受信することを特徴とするプログラムが記録された請求項６９記載の記録媒体。

【請求項７２】 上記所定のプログラムを所定の暗号化

鍵で暗号化した暗号化プログラムデータが記録された記録媒体を再生する再生ステップを備え、

上記暗号化プログラムデータ受信ステップは、上記再生ステップで再生された上記暗号化プログラムデータを受信することを特徴とするプログラムが記録された請求項６９記載の記録媒体。

【請求項７３】　上記暗号化プログラムデータ受信ステップは、上記所定のプログラムのプログラムデータから所定の演算によって算出された第１の検証データと、上記所定の演算をするプログラムである検証プログラムとが上記所定の暗号化鍵で暗号化された暗号化検証データと、暗号化検証プログラムとを含んだ上記暗号化プログラムデータを受信することを特徴とするプログラムを記録した請求項６９記載の記録媒体。

【請求項７４】　上記復号ステップは、上記暗号化プログラムデータを復号する際、上記暗号化検証データと、上記暗号化検証プログラムとを上記所定の復号鍵を用いて上記第１の検証データと、上記検証プログラムに復号し、

上記記憶ステップは、上記記憶手段に上記復号ステップで復号された上記第１の検証データと、上記検証プログラムとを記憶し、

上記制御ステップで、上記所定のプログラムを実行する前に、上記検証プログラムに基づいて、上記記憶手段に記憶された上記所定のプログラムのプログラムデータから第２の検証データを算出する検証データ算出ステップと、

上記検証データ算出ステップで算出された上記第２の検証データと、上記記憶手段に記憶されている上記第１の検証データとを比較する検証データ比較ステップとを備え、

上記プログラム読み出しステップは、上記検証データ比較ステップによって比較された上記第１の検証データと、上記第２の検証データとが一致したことに応じて、上記記憶手段に記憶されている上記所定のプログラムを読み出すことを特徴とするプログラムを記録した請求項７３記載の記録媒体。

【請求項７５】　情報処理装置の所定のデータ処理を行うデータ処理手段を集積化した回路素子であって、

所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信手段と、

上記暗号化プログラムデータ受信手段で受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記所定のプログラムに復号する復号手段と、

上記復号手段で上記暗号化プログラムデータから復号された上記所定のプログラムを記憶する記憶手段と、

上記記憶手段に記憶された上記所定のプログラムを読み出すプログラム読み出し手段と、

上記プログラム読み出し手段によって読み出された上記所定のプログラムに基づいて、上記データ処理手段における所定のデータ処理動作を制御する第１の制御手段と、

上記復号手段で復号された上記所定のプログラム及び上記記憶手段に記憶された上記所定のプログラムの外部装置からの取り出しを制限する取り出し制限手段とを集積化してなることを特徴とする回路素子。

【請求項７６】　上記暗号化プログラムデータが記憶された暗号化プログラムデータ記憶手段を有する情報処理装置に備えられ、

上記第１の制御手段は、上記暗号化プログラムデータ記憶手段に記憶されている上記暗号化プログラムデータを読み出し、

上記暗号化プログラムデータ受信手段は、上記第１の制御手段によって読み出された上記暗号化プログラムデータを受信することを特徴とする請求項７５記載の回路素子。

【請求項７７】　第２の制御手段を有する上記情報処理装置に備えられ、

上記第２の制御手段は、上記暗号化プログラムデータ記憶手段に記憶されている上記暗号化プログラムデータを読み出し、

上記暗号化プログラムデータ受信手段は、上記第２の制御手段によって読み出された上記暗号化プログラムデータを受信することを特徴とする請求項７５記載の回路素子。

【請求項７８】　上記暗号化プログラムデータ受信手段は、外部装置から送信される暗号化プログラムデータを受信することを特徴とする請求項７５記載の回路素子。

【請求項７９】　上記所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータが記録された記録媒体を再生する再生手段を有する情報処理装置に備えられ、

上記第１の制御手段は、上記記録媒体を再生させるよう上記再生手段を制御し、

上記暗号化プログラムデータ受信手段は、上記再生手段で再生された上記暗号化プログラムデータを受信することを特徴とする請求項７５記載の回路素子。

【請求項８０】　上記暗号化プログラムデータ受信手段で受信される暗号化プログラムデータは、上記所定のプログラムのプログラムデータから所定の演算によって算出された第１の検証データと、上記所定の演算をするプログラムである検証プログラムとが上記所定の暗号化鍵で暗号化された暗号化検証データと、暗号化検証プログラムとを含むことを特徴とする請求項７５記載の回路素子。

【請求項８１】　上記復号手段は、上記暗号化プログラムデータを復号する際、上記暗号化検証データと、上記暗号化検証プログラムとを上記所定の復号鍵を用いて上記第１の検証データと、上記検証プログラムに復号し、

19

上記記憶手段は上記復号手段で復号された上記第１の検証データと、上記検証プログラムとを記憶し、
上記第１の制御手段は、上記所定のプログラムを実行する前に、上記検証プログラムに基づいて、上記記憶手段に記憶された上記所定のプログラムのプログラムデータから第２の検証データを算出し、算出された上記第２の検証データと、上記記憶手段に記憶されている上記第１の検証データとを比較し、
上記プログラム読み出し手段は、上記第１の制御手段によって比較された上記第１の検証データと、上記第２の検証データとが一致したことに応じて、上記記憶手段に記憶されている上記所定のプログラムを読み出すことを特徴とする請求項８０記載の回路素子。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報処理装置のプログラム更新に関するものであり、詳しくはプログラムの更新、又は、プログラムのロード時に、プログラムデータの漏洩を阻止することでプログラムが改竄されることを防止する情報処理装置、プログラムロード方法、記録媒体、プログラム更新方法及び回路素子に関する。

【０００２】

【従来の技術】ＤＶＤ（Digital Versatile Disc）は、映画1本分相当の映像と音声のデジタルデータを記録できる記録容量を持つ光ディスクであり、ＲＯＭ(DVD-ROM：DVD-Read Only Memory)として利用されている。

【０００３】ＤＶＤ－ＲＯＭは劣化のないデジタルデータを記録しているため、記憶されているデジタルデータの違法コピーや、違法利用を防止するためにいくつかのプロテクト機能が備えられている。

【０００４】例えば、ＤＶＤ－ＲＯＭを再生する際のプロテクト機能としては、リージョナルコード（RC：Regional Code）による再生制限がある。リージョナルコードとは、世界を６つに分けて、それぞれに付与した番号のことである。例えば、アメリカのリージョナルコードは”１”であり、日本のリージョナルコードは”２”である。

【０００５】リージョナルコードは、ＤＶＤ－ＲＯＭとＤＶＤ－ＲＯＭを再生するＤＶＤ－ＲＯＭドライブ又はＤＶＤ再生アプリケーションにそれぞれ与えられ、それぞれのリージョナルコードが一致しないと、再生をすることができないようになっている。例えば、日本で生産されたＤＶＤ－ＲＯＭドライブにはリージョナルコード”２”が与えられているため、アメリカで生産されたリージョナルコード”１”のＤＶＤ－ＲＯＭを再生することはできない。これは、映画などのコンテンツ制作者を保護する目的で付けられたプロテクト機能である。

【０００６】また、ＤＶＤ－ＲＯＭには、デジタルコピーを防止するプロテクト機能がある。これは、ＣＳＳ（Content Scrambling System）と呼ばれており、ファイル自体は、ハードディスクなどにコピー可能であるが、コピーしたファイルを再生させると暗号化されたデータであるため、ＭＰＥＧ（Moving Picture Experts Group）データのデコードをできないようにさせることでデジタルコピーを防止している。

20

【０００７】他に、ＤＶＤ－ＲＯＭには、アナログ出力されたデータのコピーを防止するプロテクト機能や、デジタル機器間でのデジタルデータのコピー世代を管理し制限するプロテクト機能などがある。

【０００８】このようなプロテクト機能は、ＤＶＤ－ＲＯＭドライブ内の所定のＲＯＭに書き込まれたファームウエアと呼ばれるプログラムによって実行される。ファームウエアは、ハードウエアを直接的に制御するソフトウエアをＲＯＭに書き込み、ハードウエア内に組み込んだものである。

【０００９】ＤＶＤ－ＲＯＭドライブの所定のＲＯＭに書き込まれたプロテクト機能を実行するファームウエアによって、不正に作成されたＤＶＤ－Ｖｉｄｅｏを排除することができる。

【００１０】ところで、一般に、このようなファームウエアを書き換えたり変更することは困難であるが、例えば、ＰＣ（Personal Computer）などに接続し、ＰＣの制御によって作動するＤＶＤ－ＲＯＭドライブなどでは、ＰＣのＯＳ（Operating System）がアップデートされることに伴ってファームウエアもアップデートする必要が生じてくる。したがって、このような、ＤＶＤ－ＲＯＭではファームウエアの更新を可能とするような構成となっている。

【００１１】また、ＰＣと、ＤＶＤ－ＲＯＭドライブとの接続の相性がよくない場合なども、ＤＶＤ－ＲＯＭドライブのファームウエアを更新することで改善させることができる。

【００１２】ファームウエアを更新可能とするには、当該ファームウエアを格納するＲＯＭにデータの電気的消去が可能なプログラマブルＲＯＭであるＥＥＰＲＯＭ（Electrically Erasable Programmable Read-Only Memory）などの、いわゆるフラッシュメモリが用いられる。

【００１３】

【発明が解決しようとする課題】しかし、このようなファームウエアを更新する場合、ファームウエアをＤＶＤ－ＲＯＭドライブのメーカが提供するホームページなどからインターネットで簡単にダウンロードできるため、ユーザはファームウエアを簡単に入手することができる。

【００１４】さらに、ユーザは入手したファームウエアを改竄し、ＤＶＤ－ＲＯＭドライブの所定のフラッシュメモリに格納することで、上述したＤＶＤ－ＲＯＭのプロテクト機能を無効化させるといった問題がある。

【００１５】上述したファームウエアに限らずプログラ

ムの改竄は、プログラムの転送を必要とする装置には必ず生ずる問題である。改竄プログラムを使用した装置は、期待される動作と異なる動作をしたり、さらに最悪の場合には故障をしてしまうといった問題をも含んでいる。

【００１６】そこで、本発明は上述したような問題を解決するために案出されたものであり、プログラムの更新、又は、プログラムのロード時に、外部にプログラムデータが漏洩することによって生ずるプログラムの改竄を阻止し、デジタルデータの不正利用を防止する情報処理装置、プログラムロード方法、記録媒体、プログラム更新方法及び回路素子を提供することを目的とする。

【００１７】

【課題を解決するための手段】上述の目的を達成するために、本発明に係る情報処理装置は、所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信手段と、上記暗号化プログラムデータ受信手段で受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記所定のプログラムに復号する復号手段と、上記復号手段で上記暗号化プログラムデータから復号された上記所定のプログラムを記憶する記憶手段と、上記記憶手段に記憶された上記所定のプログラムを読み出すプログラム読み出し手段と、上記読み出し手段によって読み出された上記所定のプログラムに基づいて当該情報処理装置の所定の動作を制御する制御手段とを備えることを特徴とする。

【００１８】上述の目的を達成するために、本発明に係るプログラムロード方法は、情報処理装置に所定のプログラムをロードするためのプログラムロード方法であって、上記所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信ステップと、上記暗号化プログラムデータ受信ステップで受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記所定のプログラムに復号する復号ステップと、上記復号ステップで上記暗号化プログラムデータから復号された上記所定のプログラムを記憶手段に記憶する記憶ステップと、上記記憶手段に記憶された上記所定のプログラムを読み出すプログラム読み出しステップと、上記読み出しステップによって読み出された上記所定のプログラムに基づいて当該情報処理装置の所定の動作を制御する制御ステップとを備えることを特徴とする。

【００１９】上述の目的を達成するために、本発明に係る記録媒体は、情報処理装置に所定のプログラムをロードするためのプログラムを記録した記録媒体であって、上記所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信ステップと、上記暗号化プログラムデータ受信ステップで受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記所定のプログラムに復号する復号ステップと、上記復号ステップで上記暗号化プログラムデータから復号された上記所定のプログラムを記憶手段に記憶する記憶ステップと、上記記憶手段に記憶された上記所定のプログラムを読み出すプログラム読み出しステップと、上記読み出しステップによって読み出された上記所定のプログラムに基づいて当該情報処理装置の所定の動作を制御する制御ステップとを備えることを特徴とするプログラムが記録されている。

【００２０】上述の目的を達成するために、本発明に係る情報処理装置は、第１のプログラムが記憶された記憶手段と、上記記憶手段に記憶されている上記第１のプログラムを読み出し、読み出した上記第１のプログラムに基づいて当該情報処理装置の所定の動作を制御する制御手段とを有する制御部を備えた情報処理装置であって、上記制御部は、上記第１のプログラムの更新を要求するプログラム更新要求に応じて、第２のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信手段と、上記暗号化プログラムデータ受信手段で受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記第２のプログラムに復号する復号手段と、上記復号手段で上記暗号化プログラムデータから復号された第２のプログラムを、上記記憶手段に書き込むプログラム書き込み手段と、上記復号手段で復号された第２のプログラム及び上記記憶手段に書き込まれた第２のプログラムの外部装置からの取り出しを制限する取り出し制限手段とを備えることを特徴とする。

【００２１】上述の目的を達成するために、本発明に係るプログラム更新方法は、第１のプログラムが記憶された記憶手段と、上記記憶手段に記憶されている上記第１のプログラムを読み出し、読み出した上記第１のプログラムに基づいて当該情報処理装置の所定の動作を制御する制御手段とを有する制御部を備えた情報処理装置のプログラム更新方法であって、上記第１のプログラムの更新を要求するプログラム更新要求に応じて、第２のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信ステップと、上記受信した暗号化プログラムデータを所定の復号鍵を用いて上記第２のプログラムに復号する復号ステップと、上記復号された第２のプログラムの外部装置からの取り出しを制限する取り出し制限ステップと、上記暗号化プログラムデータから復号された第２のプログラムを、上記記憶手段に書き込むプログラム書き込みステップとを備えることを特徴とする。

【００２２】上述の目的を達成するために、本発明に係る記録媒体は、第１のプログラムが記憶された記憶手段と、上記記憶手段に記憶されている上記第１のプログラムを読み出し、読み出した上記第１のプログラムに基づいて所定の動作を制御する制御手段とを有する制御部を備えた情報処理装置の上記第１のプログラムを更新する

ためのプログラムを記録した記録媒体であって、上記第１のプログラムの更新を要求するプログラム更新要求に応じて、第２のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信ステップと、上記受信した暗号化プログラムデータを所定の復号鍵を用いて上記第２のプログラムに復号する復号ステップと、上記復号された第２のプログラムの外部装置からの取り出しを制限する取り出し制限ステップと、上記暗号化プログラムデータから復号された第２のプログラムを上記記憶手段に書き込むプログラム書き込みステップとを備えることを特徴とするプログラムが記録されている。

【００２３】上述の目的を達成するために、本発明に係る回路素子は、第１のプログラムが記憶された記憶手段と、上記記憶手段に記憶されている上記第１のプログラムを読み出し、読み出した上記第１のプログラムに基づいて情報処理装置の所定の動作を制御する制御手段とを集積化した回路素子であって、上記第１のプログラムの更新を要求するプログラム更新要求に応じて、第２のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信手段と、上記暗号化プログラムデータ受信手段で受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記第２のプログラムに復号する復号手段と、上記復号手段で上記暗号化プログラムデータから復号された第２のプログラムを、上記記憶手段に書き込むプログラム書き込み手段と、上記復号手段で復号された第２のプログラム及び上記記憶手段に書き込まれた第２のプログラムの外部装置からの取り出しを制限する取り出し制限手段とを集積化してなることを特徴とする。

【００２４】上述の目的を達成するために、本発明に係る情報処理装置は、第１のプログラムが記憶された記憶手段と、上記記憶手段に記憶されている上記第１のプログラムを読み出し、読み出した上記第１のプログラムに基づいて当該情報処理装置の所定の動作を制御する制御手段とを有する制御部を備えた情報処理装置であって、上記第１のプログラムの更新を要求するプログラム更新要求に応じて、第２のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信手段と、上記暗号化プログラムデータ受信手段で受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記第２のプログラムに復号する復号手段と、上記復号手段で上記暗号化プログラムデータから復号された上記第２のプログラムを上記制御部に送信するプログラム送信手段とを備え、上記制御部は、上記送信手段によって送信された上記第２のプログラムを受信するプログラム受信手段と、上記プログラム受信手段で受信した上記第２のプログラムを上記記憶手段に書き込むプログラム書き込み手段とを有することを特徴とする。

【００２５】上述の目的を達成するために、本発明に係るプログラム更新方法は、第１のプログラムが記憶された記憶手段と、上記記憶手段に記憶されている上記第１のプログラムを読み出し、読み出した上記第１のプログラムに基づいて当該情報処理装置の所定の動作を制御する制御手段とを有する制御部を備えた情報処理装置のプログラム更新方法であって、上記第１のプログラムの更新を要求するプログラム更新要求に応じて、第２のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信ステップと、上記暗号化プログラムデータ受信ステップで受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記第２のプログラムに復号する復号ステップと、上記復号ステップで上記暗号化プログラムデータから復号された上記第２のプログラムを上記制御部に送信するプログラム送信ステップとを備え、上記プログラム送信ステップによって上記制御部に送信された上記第２のプログラムを受信するプログラム受信ステップと、上記プログラム受信ステップで受信した上記第２のプログラムを上記記憶手段に書き込むプログラム書き込みステップとを有することを特徴とする。

【００２６】上述の目的を達成するために、本発明に係る記録媒体は、第１のプログラムが記憶された記憶手段と、上記記憶手段に記憶されている上記第１のプログラムを読み出し、読み出した上記第１のプログラムに基づいて当該情報処理装置の所定の動作を制御する制御手段とを有する制御部を備えた情報処理装置の上記第１のプログラムを更新するためのプログラムを記録した記録媒体であって、上記第１のプログラムの更新を要求するプログラム更新要求に応じて、第２のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信ステップと、上記暗号化プログラムデータ受信ステップで受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記第２のプログラムに復号する復号ステップと、上記復号ステップで上記暗号化プログラムデータから復号された上記第２のプログラムを上記制御部に送信するプログラム送信ステップとを備え、上記プログラム送信ステップによって上記制御部に送信された上記第２のプログラムを受信するプログラム受信ステップと、上記プログラム受信ステップで受信した上記第２のプログラムを上記記憶手段に書き込むプログラム書き込みステップとを有することを特徴とするプログラムが記録されている。

【００２７】上述の目的を達成するために、本発明に係る情報処理装置は、所定のデータ処理を行うデータ処理部を備えた情報処理装置であって、上記データ処理部は、所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信手段と、上記暗号化プログラムデータ受信手段で受信した上記暗号化プログラムデータを所定の復号鍵を

用いて上記所定のプログラムに復号する復号手段と、上記復号手段で上記暗号化プログラムデータから復号された上記所定のプログラムを記憶する記憶手段と、上記記憶手段に記憶された上記所定のプログラムを読み出すプログラム読み出し手段と、上記プログラム読み出し手段によって読み出された上記所定のプログラムに基づいて、当該データ処理部における所定のデータ処理動作を制御する第１の制御手段と、上記復号手段で復号された上記所定のプログラム及び上記記憶手段に記憶された上記所定のプログラムの外部装置からの取り出しを制限する取り出し制限手段とを有することを特徴とする。

【００２８】上述の目的を達成するために、本発明に係るプログラムロード方法は、所定のデータ処理を行うデータ処理部を備えた情報処理装置の上記データ処理部でのプログラムロード方法であって、所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信ステップと、上記プログラムデータ受信ステップで受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記所定のプログラムに復号する復号ステップと、上記復号された上記所定のプログラムの外部装置からの取り出しを制限する取り出し制限ステップと、上記復号ステップで上記暗号化プログラムデータから復号された上記所定のプログラムを記憶手段に記憶させる記憶ステップと、上記記憶手段に記憶された上記所定のプログラムを読み出すプログラム読み出しステップと、上記プログラム読み出しステップによって読み出された上記所定のプログラムに基づいて、当該データ処理部における所定のデータ処理動作を制御する制御ステップと有することを特徴とする。

【００２９】上述の目的を達成するために、本発明に係る記録媒体は、所定のデータ処理を行うデータ処理部を備えた情報処理装置の上記データ処理部で所定のプログラムをロードするためのプログラムを記録した記録媒体であって、上記所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信ステップと、上記プログラムデータ受信ステップで受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記所定のプログラムに復号する復号ステップと、上記復号された上記所定のプログラムの外部装置からの取り出しを制限する取り出し制限ステップと、上記復号ステップで上記暗号化プログラムデータから復号された上記所定のプログラムを記憶手段に記憶する記憶ステップと、上記記憶手段に記憶された上記所定のプログラムを読み出すプログラム読み出しステップと、上記プログラム読み出しステップによって読み出された上記所定のプログラムに基づいて、上記データ処理部における所定のデータ処理動作を制御する制御ステップと有することを特徴とするプログラムが記録されている。

【００３０】上述の目的を達成するために、本発明に係

る回路素子は、情報処理装置の所定のデータ処理を行うデータ処理手段を集積化した回路素子であって、所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信手段と、上記暗号化プログラムデータ受信手段で受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記所定のプログラムに復号する復号手段と、上記復号手段で上記暗号化プログラムデータから復号された上記所定のプログラムを記憶する記憶手段と、上記記憶手段に記憶された上記所定のプログラムを読み出すプログラム読み出し手段と、上記プログラム読み出し手段によって読み出された上記所定のプログラムに基づいて、上記データ処理手段における所定のデータ処理動作を制御する第１の制御手段と、上記復号手段で復号された上記所定のプログラム及び上記記憶手段に記憶された上記所定のプログラムの外部装置からの取り出しを制限する取り出し制限手段とを集積化してることを特徴とする。

【００３１】

【発明の実施の形態】以下、本発明に係る情報処理装置、プログラムロード方法、記録媒体、プログラム更新方法及び回路素子の実施の形態を図面を参照にして詳細に説明する。

【００３２】まず、図１に第１の実施の形態として示すＤＶＤ－ＲＯＭドライブの構成について説明をする。

【００３３】ＤＶＤ－ＲＯＭドライブは、ＤＶＤ－ＲＯＭ（Digital Versatile Disc-ReadOnly Memory）１を所定の箇所に装着し、装着したＤＶＤ－ＲＯＭ１を再生する装置である。ＤＶＤ－ＲＯＭドライブは、ＰＣ（Personal Computer）１０に接続され、装着したＤＶＤ－ＲＯＭ１の再生動作などの各種動作は、接続されたＰＣ１０によって制御される。

【００３４】ＤＶＤ－ＲＯＭドライブは、光学ピックアップユニット２と、スピンドルモータ３と、リードプロセッサ４と、光学ピックアップユニットドライバ５と、スピンドルモータドライバ６と、ＤＶＤデコーダ７と、バッファメモリ８と、ＣＰＵ９とを備える。

【００３５】光学ピックアップユニット２は、図示しないが、所定の波長のレーザ光を出射するレーザダイオードと、レーザダイオードから出射された所定の波長のレーザ光をＤＶＤ－ＲＯＭ１のデータ記録面に集光して出射し、ＤＶＤ－ＲＯＭ１のデータ記録面で反射された反射光を集光して出射する対物レンズと、所定の制御信号に応じて上記対物レンズを搭載し対物レンズを駆動させフォーカス調整及びトラッキング調整を行う２軸アクチュエータと、ＤＶＤ－ＲＯＭ１のデータ記録面で反射された反射光を受光し電気信号に変換することでデータ記録面のピットの有無を検出するフォトディテクタとを備えている。フォトディテクタで検出された電気信号は、一般にＲＦ（Radio Frequency）信号と呼ばれている。

【００３６】また、当該光学ピックアップユニット２に

27

は、当該光学ピックアップユニット２をＤＶＤ－ＲＯＭ１の半径方向に駆動させるスレッドモータが備えられている。

【００３７】さらにまた、当該ＤＶＤ－ＲＯＭドライブが、図示しないディスクトレイにＤＶＤ－ＲＯＭ１を載せてローディングする機構を備えている場合は、このディスクトレイを動作させるローディングモータもこの光学ピックアップユニット２に備えられていてもよい。

【００３８】スピンドルモータ３は、装着されたＤＶＤ－ＲＯＭ１を回転駆動させるモータである。

【００３９】リードプロセッサ４は、光学ピックアップユニット２が備えるフォトディテクタで検出されたＲＦ信号からＤＶＤ読み出し用ＥＦＭ＋（Eight to Fourteen Plus Modulation）信号と、フォーカスサーボ用のＦＥ（Focus Error）信号、トラッキングサーボ用のＴＥ（Tracking Error）信号、Ｐｕｌｌ－ｉｎ信号を生成し、後述するＤＶＤデコーダ７のサーボ制御部１２に送出する。

【００４０】光学ピックアップユニットドライバ５は、所定の制御信号に応じて上述の光学ピックアップユニット２の図示しない２軸アクチュエータ、スレッドモータ、ローディングモータをそれぞれ駆動させるドライバＩＣ（Integrated Circuit）である。

【００４１】スピンドルモータドライバ６は、所定の制御信号に応じて上述のスピンドルモータ３を駆動させるドライバＩＣである。

【００４２】ＤＶＤデコーダ７は、ＤＶＤ信号処理部１１と、サーボ制御部１２と、ディスク回転制御部１３と、メモリ制御部１４と、ＡＴＡＰＩ（AT Attachment with Packet Interface）１５と、ＣＰＵ　Ｉ／Ｆ１６とを備えている。

【００４３】ＤＶＤ信号処理部１１は、ＲＳ－ＰＣ復号器、アドレス検出のためのＩＤ処理、８／１６変換回路、記録可能メディアか否かを判定するためのＷｏｂｂｌｅディテクタを備えている。

【００４４】サーボ制御部１２は、リードプロセッサ４から送信されたＦＥ信号、ＴＥ信号、Ｐｕｌｌ－ｉｎ信号に応じて、光学ピックアップユニット２の２軸アクチュエータ、スレッドモータを駆動制御するための制御信号を生成し、光学ピックアップユニットドライバ５へ送出する。

【００４５】ディスク回転制御部１３は、ＤＶＤ－ＲＯＭ１を装着したスピンドルモータ３の回転を制御する制御信号を生成し、スピンドルモータドライバ６へ送出する。

【００４６】メモリ制御部１４は、バッファメモリ８へデータの書き込み、読み出しを制御する。

【００４７】ＡＴＡＰＩ１５は、ＰＣ１０と、当該ＤＶＤ－ＲＯＭドライブとを接続し、データのやり取りを行うためのインターフェースである。

28

【００４８】なお、ＰＣ１０と接続するためのインターフェースは、このＡＴＡＰＩ１５以外にも、例えば、ＳＣＳＩ（Small Computer System Interface）、ＵＳＢ（Universal Serial Bus）、ＩＥＥＥ（Institute of Electrical and Electronics Engineers）１３９４などであってもよい。

【００４９】ＣＰＵ　Ｉ／Ｆ１６は、当該ＤＶＤデコーダ７とＣＰＵ９とを接続し、ＣＰＵ９から当該ＤＶＤデコーダ７を制御するためのインターフェースである。また、ＣＰＵ　Ｉ／Ｆ１６は、バッファメモリ８に記憶されているデータを読み出したり、バッファメモリ８にデータを書き込んだりする。

【００５０】バッファメモリ８は、例えば、ＤＲＡＭ（Dynamic Random-Access Memory）などのランダムアクセス可能なメモリであり、ＤＶＤ信号処理部１１から送出されたデータ、ＰＣ１０から送出されたデータ、ＣＰＵ９から送出されたデータを一時的にを記憶する。

【００５１】ＣＰＵ９は、ＣＰＵ　Ｉ／Ｆ１６でＤＶＤデコーダ７と接続され、ＤＶＤ－ＲＯＭドライブの各機能を統括的に制御する。ＣＰＵ９の構成及び機能については、後で詳細に説明をする。

【００５２】ＰＣ１０は、ＤＶＤ－ＲＯＭドライブと、ＤＶＤデコーダ７のＡＴＡＰＩ１５などで接続され、ＤＶＤ－ＲＯＭドライブの動作、例えば、再生、停止、データ検索などを、所定のコマンドを入力することで制御する。ユーザは、ＰＣ１０を介して、ＤＶＤ－ＲＯＭ１の各種データを利用することができる。

【００５３】続いて、ＣＰＵ９の構成について詳細に説明をする。

【００５４】ＣＰＵ９は、ＣＰＵコア２０と、ブートＲＯＭ２１と、フラッシュＲＯＭ２２と、ＲＡＭ２３と、入力／出力ポート２４と、書き込みタイミング制御用タイマー２５と、割り込み制御回路２６と、シリアル通信回路２７と、３２ｂｉｔバス２８、１６ｂｉｔバス２９と、ブリッジ回路３０と、外部バスコントローラ３１とを備えている。

【００５５】ＣＰＵコア２０は、ＣＰＵ９における中心部分で四則演算や比較判断をする論理演算装置や加算回路、レジスタなどを備えている。

【００５６】ブートＲＯＭ２１は、例えば、データの電気的消去が可能なプログラマブルＲＯＭであるＥＥＰＲＯＭ（Electrically Erasable Programmable Read-Only Memory）などのいわゆるフラッシュメモリである。

【００５７】ブートＲＯＭ２１には、フラッシュＲＯＭ２２に記憶されたプログラムをアップデートする際に起動させるブートプログラムを格納している。このブートプログラムを起動させるには、例えば、ＣＰＵ９に設けられた端子に所定の電圧を印加することで実行する。上述の端子に所定の電圧が印加されると、ブートプログラムが先頭アドレスから読み出されブートプログラムが実

行される。

【００５８】またブートＲＯＭ２１は、暗号化され送信されたファームウエアを解読するために用いる共通鍵をプログラムとして格納すると共に、この共通鍵を用いて暗号化されたファームウエアを解読する暗号解読アルゴリズムを格納した暗号化処理部２１ａを備えている。

【００５９】フラッシュＲＯＭ２２は、ブートＲＯＭ２１と同様に、例えば、データの電気的消去が可能なプログラマブルＲＯＭであるＥＥＰＲＯＭなどのいわゆるフラッシュメモリである。

【００６０】フラッシュＲＯＭ２２には、ファームウエアが格納され、当該ＤＶＤ－ＲＯＭドライブの再生制限をするプログラムであるファームウエアが格納される。フラッシュＲＯＭ２２に格納されたファームウエアは、ＤＶＤ－ＲＯＭドライブの所定の動作、例えば、ＤＶＤ－ＲＯＭ１の再生制限や、デジタルコピーの制限をするプログラムである。

【００６１】また、フラッシュＲＯＭ２２に代えてＴＭＲ（Tunneling Magneto Resistive）素子を用いたＭＲＡＭ（Magnetic Random Access Memory）を使用してもよい。ＭＲＡＭは、磁気によってデータを記憶するメモリであるためデータのオーバーライトが可能である。したがって、ファームウエアを更新する際に、ＭＲＡＭに記憶されているデータ、つまり更新前のファームウエアの消去動作が不要となる。

【００６２】ここで、図２を用いて、共通鍵について説明をする。

【００６３】図２に示すように、例えば、平文データを暗号化する際は所定の暗号化鍵を用いて暗号化データに変換し、再び暗号化データを復号する際は所定の復号鍵を用いて平文データとする。

【００６４】言い換えると、暗号化鍵は、平文データや情報を暗号化する時に用いられ、復号鍵は、暗号化されたデータや情報をもとの平文データや情報に戻す時に用いられる。

【００６５】共通鍵とは、上述のようにデータを暗号化する際に用いる暗号化鍵と、暗号化されたデータを復号する際に用いる復号鍵とが共通である鍵のことである。この共通鍵の情報は、公開されず秘密にしておくことから秘密鍵とも呼ばれている。

【００６６】なお、ブートＲＯＭ２１及びフラッシュＲＯＭ２２は２つの異なるフラッシュＲＯＭを用いるように記載しているが、これを１つのフラッシュＲＯＭとし、このフラッシュＲＯＭの記憶領域をブート領域、プログラム領域のように分割するようにしてもよい。

【００６７】ＲＡＭ２３は、記憶内容維持のためのリフレッシュ動作が不要で高速アクセス可能なＳＲＡＭ（Static Random Access Memory）などであり、フラッシュＲＯＭ２２に格納されているファームウエアをアップデートする際にデータ及びアップデート用プログラムの展開領域となる。

【００６８】一般にフラッシュメモリでは、当該フラッシュメモリに記憶されているデータをアップデートする際、自分自身でプログラムを実行することができない。したがって、ファームウエアのアップデート時には、バッファメモリ８から転送されるファームウエアのデータと共にアップデート用のアップデート関数がブートＲＯＭ２１からＲＡＭ２３にコピーされる。

【００６９】入力／出力ポート２４は、当該ＣＰＵ９にデータの入力ポート、及び、当該ＣＰＵ９から出力するデータの出力ポートである。

【００７０】書き込みタイミング制御用タイマー２５は、フラッシュＲＯＭ２２のファームウエアをアップデートする際の書き込みのタイミングを制御する。

【００７１】割り込み制御回路２６は、所定の割り込み発生に応じて現在実行中の処理を中断し割り込みプログラムを実行させるよう制御する回路である。

【００７２】シリアル通信回路２７は、シリアルデータを送受信するインターフェースである。

【００７３】３２ｂｉｔバス２８は、一度に３２ｂｉｔのデータを伝送可能なバスである。

【００７４】１６ｂｉｔバス２９は、一度に１６ｂｉｔのデータを伝送可能なバスである。

【００７５】ブリッジ回路３０は、３２ｂｉｔバス２８と、１６ｂｉｔバス２９とを接続する回路である。

【００７６】外部バスコントローラ３１は、当該ＣＰＵ９と外部装置であるＤＶＤデコーダ７との間で伝送されるデータを監視し、ＤＶＤデコーダ７とのデータ入出力を制御をする。また、外部バスコントローラ３１は、当該ＣＰＵ９内のブートＲＯＭ２１及びフラッシュＲＯＭ２２に格納されているプログラムとＲＡＭ２３をユーザレベルでは参照できないような保護機能を備えている。これにより、共通鍵、暗号化処理部２１ａ及び復号されたファームウエアをＣＰＵ９から取り出すことを制限することができる。

【００７７】続いて、図３に示すフローチャートを用いて、フラッシュＲＯＭ２２に記憶されたファームウエアをアップデートする際の動作について説明をする。

【００７８】まず、ステップＳ１において、ＣＰＵ９のＣＰＵコア２０は、ブート端子にかけられた電圧がＨＩＧＨレベル（High Level）であった場合、工程をステップＳ２へと進め、ＬＯＷレベル（Low Level）であった場合、工程をステップＳ４へと進める。

【００７９】ステップＳ２からの工程はフラッシュＲＯＭ２２に記憶されているプログラムを実行する工程であり、ステップＳ４からの工程はブートＲＯＭ２１に記憶されいるブートプログラムを起動させ、ファームウエアをアップデートする工程である。

【００８０】ステップＳ２において、ＣＰＵコア２０は、フラッシュＲＯＭ２２のプログラム、例えば、ファ

ームウエアなどが記録されているプログラム領域の先頭アドレスへアクセスする。

【００８１】ステップＳ３において、ＣＰＵコア２０はアクセスしたフラッシュＲＯＭ２２のプログラム領域に記憶されているプログラムに応じて、ＤＶＤ－ＲＯＭ１に対して通常処理、例えば、再生処理、データ検索処理などを実行する。

【００８２】ステップＳ４において、ブート端子にＬＯＷレベルの電圧がかかったことに応じて、ブートＲＯＭ２１のブートプログラムが記憶されているブート領域の先頭アドレスがＣＰＵコア２０に読み込まれ、ブートプログラムが起動する。

【００８３】ステップＳ５において、ＣＰＵコア２０は、当該ＤＶＤ－ＲＯＭドライブの全ポートを初期化する。これによりＤＶＤ－ＲＯＭドライブのメカ系及び電気系の破壊が防止される。

【００８４】ステップＳ６において、ＣＰＵコア２０は、ＰＣ１０からＮｏｔ　Ｒｅａｄｙ状態で実行可能なコマンドが入力されたかどうかを判断する。ここでいうＮｏｔＲｅａｄｙ状態とは、当該ＤＶＤ－ＲＯＭドライブにＤＶＤ－ＲＯＭ１が装着されていない、或いはＤＶＤ－ＲＯＭ１がＣＰＵ９に認識されていない状態を示し、Ｎｏｔ　Ｒｅａｄｙ状態で実行可能なコマンドとは、ＤＶＤ－ＲＯＭ１が認識されていないくても実行可能なコマンドである。例えば、ＤＶＤ－ＲＯＭ１から所定のデータを読み出せというようなコマンドは、Ｎｏｔ　Ｒｅａｄｙでは実行不可能なコマンドである。

【００８５】Ｎｏｔ　Ｒｅａｄｙ状態で実行可能なコマンドが入力された場合は工程をステップＳ８へと進め、実行不可能なコマンドが入力された場合は工程をステップＳ７へと進める。

【００８６】ステップＳ７において、ＣＰＵコア２０は、Ｎｏｔ　Ｒｅａｄｙ状態で実行不可能なコマンドが入力されたことに応じて、Ｃｈｅｃｋ　ＣｏｎｄｉｔｉｏｎＳｔａｔｕｓでコマンドを完了させ、工程を再びステップＳ６へと戻す。

【００８７】ステップＳ８において、ＣＰＵコア２０は、フラッシュＲＯＭ２２のプログラム更新を指示するＷｒｉｔｅバッファコマンド（Write Buffer Command）とは異なるコマンドがＰＣ１０から送信された場合は工程をステップＳ９へと進め、Ｗｒｉｔｅバッファコマンドが送信された場合は工程をステップＳ１０へと進める。

【００８８】ステップＳ９において、ＣＰＵコア２０は、Ｗｒｉｔｅバッファコマンドとは異なるコマンドが入力されたことに応じて、入力されたコマンドを実行する。

【００８９】ＰＣ１０は、ＤＶＤ－ＲＯＭドライブにＷｒｉｔｅバッファコマンドを送信した後、アップデートするファームウエアを共通鍵で暗号化したファームウエア暗号化データをバイナリーファイルとしてＤＶＤ－ＲＯＭドライブに送信する。

【００９０】ステップＳ１０において、ＣＰＵコア２０は、Ｗｒｉｔｅバッファコマンドを受信したことに応じて、バッファメモリ８のデータ記憶領域の所定のアドレスNから２×Ｍ（Ｍは自然数）ＫＢ分の領域を確保し、ＰＣ１０から送信されるバイナリファイルを上記確保したデータ記憶領域に記憶させる。

【００９１】ＣＰＵコア２０はバイナリーファイルを受信すると、全バイナリーデータを加算してＣｈｅｃｋ　Ｓｕｍデータを生成し、バイナリーファイルと共にバッファメモリ８に記憶させる。Ｃｈｅｃｋ　Ｓｕｍデータは、送られてきたプログラムがエラーなく受信されたことを確認するためのデータで、送信された全てのデータを加算することで得られる。

【００９２】ステップＳ１１において、ＣＰＵコア２０は、ステップＳ１０でバッファメモリ８に格納したＣｈｅｃｋ　Ｓｕｍデータを検証し、送信されたファームウエア暗号化データが正しく受信されたかどうかを確認する。正しく受信されている場合は工程をステップＳ１３へと進め、正しく受信されていない場合は工程をステップＳ１２へと進める。

【００９３】ステップＳ１２において、ＣＰＵコア２０は、ステップＳ１１でのＣｈｅｃｋＳｕｍデータの検証結果から正しくバイナリファイルが送信されなかったことを、Ｃｈｅｃｋ　Ｃｏｎｄｉｔｉｏｎ　Ｓｔａｔｕｓでコマンドを完了させることでＰＣ１０に知らせ、工程を再びステップＳ６へと戻す。

【００９４】ステップＳ１３において、ＣＰＵコア２０は、ブートＲＯＭ２１に記憶されている、ファームウエアをアップデートする際に使用するアップデート（ｕｐｄａｔｅ）関数をＲＡＭ２３にコピーする。

【００９５】アップデート関数は、ＲＡＭ２３にコピーされ、ＲＡＭ２３に展開されることでファームウエアをフラッシュＲＯＭ２２にアップデートするためのアップデートプログラムとして機能する。

【００９６】続いて、図４に示すフローチャートを用いてアップデート（ｕｐｄａｔｅ）関数による処理動作について説明をする。

【００９７】ステップＳ２１において、ＣＰＵコア２０は、ＲＡＭ２３に格納されたアップデート関数の先頭アドレスにアクセスし、アップデート関数によるファームウエアのフラッシュＲＯＭ２２へのアップデートを開始する。

【００９８】ステップＳ２２において、ＣＰＵコア２０は、割り込み制御回路２６を制御して全ての割り込みプログラムの実行と、例外処理の実行を禁止する。

【００９９】さらに、ＣＰＵコア２０は、ＰＣ１０から入力されたＷｒｉｔｅバッファコマンドを受信したことに応じて、フラッシュＲＯＭ２２のファームウエア格納

領域に記憶されているデータを消去する。

【０１００】なお、フラッシュＲＯＭ２２に代えて上述したＭＲＡＭを使用した場合、当該ＭＲＡＭがデータのオーバーライトが可能なため記憶されているファームウエアの消去動作は不要となる。

【０１０１】ステップＳ２３において、ＣＰＵコア２０は、フラッシュＲＯＭ２２への書き込みタイミングを制御する書き込みタイミング制御用タイマー２５を起動させる。

【０１０２】以下、フラッシュＲＯＭ２２へデータを書き込む際は、書き込みタイミング制御用タイマー２５のタイミング制御に基づいて実行される。

【０１０３】ステップＳ２４において、ＣＰＵコア２０は、ファームウエア暗号化データのバイナリファイルが記憶されているバッファメモリ８のアドレス番号Ｎと、ファームウエアを記憶させるフラッシュＲＯＭ２２のアドレス番号０にアクセスをする。

【０１０４】ステップＳ２５において、ＣＰＵコア２０は、バッファメモリ８のアドレス番号Ｎから２ＫＢ分のアドレス番号までのデータを読み出しＲＡＭ２３にコピーする。

【０１０５】ステップＳ２６において、ＣＰＵコア２０は、ＲＡＭ２３内にコピーされた２ＫＢ分のデータを８Ｂｙｔｅごと読み出し、ブートＲＯＭ２１内の共通鍵と、暗号化処理部２１ａに記憶されている暗号解読アルゴリズムとで復号する。ＣＰＵコア２０は、復号した２ＫＢ分のデータ、つまり暗号解読されたファームウエアデータを再びＲＡＭ２３内に記憶させ展開する。

【０１０６】ステップＳ２７において、ＣＰＵコア２０は、ＲＡＭ２３内に記憶された２ＫＢのファームウエアデータをＲＡＭ２３から読み出し、フラッシュＲＯＭ２２のアドレス番号０から書き込む。

【０１０７】ステップＳ２８において、ＣＰＵコア２０は、フラッシュＲＯＭ２２に記憶させたファームウエアデータの最終アドレス番号が、２×Ｍ（Ｍは自然数）となったら工程をステップＳ３０へと進め、そうでない場合は工程をステップＳ２９へと進める。

【０１０８】ステップＳ２９において、ＣＰＵコア２０は、バッファメモリ８のアドレス番号及びフラッシュＲＯＭ２２のアドレス番号を２ＫＢ増やしたアドレス番号へアクセスをする。この工程が終了するとステップＳ２５へと戻る。

【０１０９】ステップＳ３０において、ＣＰＵコア２０は、フラッシュＲＯＭ２２への書き込みタイミングを制御する書き込みタイミング制御用タイマー２５を停止させる。

【０１１０】ステップＳ３１において、ステップＳ２８で、フラッシュＲＯＭ２２に記憶されたファームウエアデータの最終アドレス番号が２×Ｍ（Ｍは自然数）であると判定され、ステップＳ３０で書き込みタイミング制御用タイマー２５が停止されたことで、ファームウエアのフラッシュＲＯＭ２２へのアップデートが完了する。

【０１１１】ステップＳ３２において、ステップＳ３１でファームウエアのアップデートが完了したことに応じて、ＣＰＵコア２０は、フラッシュＲＯＭ２２のプログラム領域の先頭アドレスへアクセスをする。

【０１１２】ステップＳ３３において、ＣＰＵコア２０はアクセスしたフラッシュＲＯＭ２２のプログラム領域に記憶されているプログラム、つまり、更新された後のファームウエアに応じて、ＤＶＤ－ＲＯＭ１に対して通常処理、例えば、再生処理、データ検索処理などを実行する。

【０１１３】このようにして、本発明を適用したＤＶＤ－ＲＯＭドライブでは、フラッシュＲＯＭ２２に格納されているファームウエアをアップデートする際、ＰＣ１０から共通鍵を用いて暗号化したファームウエア暗号化データを、ＣＰＵ９内のブートＲＯＭ２１の暗号化処理部で共通鍵を用いて復号し、フラッシュＲＯＭ２２に書き込むことで、外部にファームウエアデータが漏洩することを防ぐことができる。

【０１１４】また、図４に示したフローチャートでは、暗号化されたファームウエア暗号化データをＰＣ１０から受信し、受信したファームウエア暗号化データを解読してフラッシュＲＯＭ２２に書き込む手法について記載しているが、ＰＣ１０から暗暗号化されていないデータが送信された場合は、図５に示すように、図４のステップＳ２５～ステップＳ２７の工程をステップＳ２５ａのように、バッファメモリ８から直接フラッシュＲＯＭ２２に直接書き込むよう変更することで実行することが可能となる。

【０１１５】次に、図６に示すフローチャートを用いて、フラッシュＲＯＭ２２にファームウエアをアップデートした結果をＰＣ１０で検証する際の処理動作について説明をする。

【０１１６】ステップＳ４１において、ＰＣ１０は、フラッシュＲＯＭ２２に格納されているファームウエアの転送を要求するＲｅａｄバッファコマンド（Read Buffer Command）をＤＶＤ－ＲＯＭドライブへ送信する。

【０１１７】ステップＳ４２において、ＰＣ１０から送信されたＲｅａｄバッファコマンドを受信したことに応じて、ＣＰＵコア２０は、フラッシュＲＯＭ２２の先頭アドレスからフラッシュＲＯＭ２２に記憶されているファームウエアの２ＫＢ分のデータを読み出す。

【０１１８】ステップＳ４３において、ＣＰＵコア２０は、読み出した２ＫＢ分のデータを、ＲＡＭ２３又は当該ＣＰＵコア２０のレジスタに書き込み記憶させる。

【０１１９】ステップＳ４４において、ＣＰＵコア２０は、ブートＲＯＭ２１の暗号化処理部２１ａを制御し、共通鍵を用いて暗号化処理部２１ａに格納されている暗号解読アルゴリズムに従って、ＲＡＭ２３又は当該ＣＰ

Ｕコア２０のレジスタに記憶されている２ＫＢ分のファームウエアデータを読み出して暗号化する。

【０１２０】ステップＳ４５において、ＣＰＵコア２０は、暗号化した２ＫＢ分のファームウエアデータをバッファメモリ８へ転送し、格納させる。

【０１２１】ステップＳ４６において、ＣＰＵコア２０は、フラッシュＲＯＭ２２に格納されているファームウエアデータを全て読み出したかどうかを検出する。ファームウエアデータを全て読み出した場合は工程をステップＳ４７へと進め、まだ、全てのファームウエアデータが読み出されていない場合は工程をステップＳ４２へと戻す。

【０１２２】ステップＳ４７において、フラッシュＲＯＭ２２に格納されているファームウエアデータが全て読み出され、暗号化されてバッファメモリ８に格納されたことに応じて、ＣＰＵコア２０は、バッファメモリ８に格納されているファームウエア暗号化データをＰＣ１０へと転送する。

【０１２３】転送されたファームウエア暗号化データは、ＰＣ１０にて暗号化されたまま、元データと比較され一致が確認される。

【０１２４】このようにしてＰＣ１０は、ＤＶＤ－ＲＯＭドライブのフラッシュＲＯＭ２２にファームウエアが確実に更新されているかどうかを検証することができる。その際に、ＣＰＵ９内でファームウエアは暗号化されＰＣ１０へと送信されるので、途中の送信経路などで平文のファームウエアを入手することはできないため、ファームウエアの解析や改竄などを防ぐことができる。

【０１２５】また、上述したように、図１の構成のＤＶＤ－ＲＯＭドライブのＣＰＵ９ではファームウエア暗号化データの復号をブートＲＯＭ２１に記憶されている暗号解読アルゴリズムというプログラムで実行しているが、図７に示すようにプログラムである暗号処理部を共通鍵暗号化処理部３２のようにハードウエア化して、ＣＰＵ９を再構成してもよい。

【０１２６】このように共通鍵暗号化処理部３２を備えるＣＰＵ９は、暗号化処理が高速となるため、ファームウエアのアップデートをより高速に実行させることができる。その際のアップデート処理の動作は、上述の図３、図４で示したフローチャートと同様の動作であるため省略をする。

【０１２７】上述の説明では、図１に示したようにＰＣ１０から送信される暗号化されたファームウエアを、ＣＰＵ９自身で解読し、ＣＰＵ９に備えられたフラッシュＲＯＭ２２にアップロードする構成となっていた。ＣＰＵ９は、暗号化されたファームウエアを解読する暗号化処理部としてブートＲＯＭ２１を備えている。

【０１２８】このように、ＣＰＵ９に備えられたブートＲＯＭ２１のように暗号化されたファームウエアの暗号を解読する暗号化処理部を図１で示したＤＶＤデコーダ

７に搭載することも可能である。暗号化処理部を搭載するようにＤＶＤデコーダ７をカスタマイズすることは、より現実的な構成であるといえる。

【０１２９】図８に第２の実施の形態として示す、ＤＶＤデコーダに暗号化されたファームウエアを解読する復号部１７を搭載させたＤＶＤ－ＲＯＭドライブについて説明をする。

【０１３０】図８に示したＤＶＤ－ＲＯＭドライブにおけるＤＶＤデコーダ７’は、ＰＣ１０から入力される暗号化されたファームウエアを解読するための復号部１７と、フラッシュＲＯＭ３８に格納された平文のファームウエアをＰＣ１０にて検証する際に暗号化する暗号化部１８とが、図１で示したＤＶＤデコーダ７に付加された構成となっている。

【０１３１】復号部１７、暗号化部１８は、暗号化の手法として、キーストリーム（鍵ストリーム）と呼ばれる乱数（擬似乱数）を暗号化鍵として平文を暗号化する共通鍵暗号の１つであるストリーム暗号を解析することができる。ストリーム暗号方式による暗号化及び復号は、１ビット又は数ビット（例えば、１バイト）の小データブロックごとに逐次行われる。

【０１３２】復号部１７は、ストリーム暗号に対応している場合は、図９に示すようにＳＥＥＤデータ格納部１７ａと、乱数生成部１７ｂと、排他的論理和演算部１７ｃとを備えている。

【０１３３】ＳＥＥＤデータ格納部１７ａは、乱数生成部１７ｂの初期入力値であり共通鍵に相当するＳＥＥＤデータを格納しており、ＣＰＵコア３６からの指示に応じて格納しているＳＥＥＤデータを乱数生成部１７ｂに出力する。

【０１３４】また、ＳＥＥＤデータ格納部１７ａに格納されるＳＥＥＤデータは、固定された値があらかじめ格納されていてもよいし、ＣＰＵコア３６から適時、設定可能としてもよい。

【０１３５】乱数生成部１７ｂは、ＳＥＥＤデータ格納部１７ａからＳＥＥＤデータが入力されたことに応じて所定のアルゴリズムで乱数を生成し、排他的論理和演算部１７ｃに出力する。

【０１３６】排他的論理和演算部１７ｃは、バッファメモリ８から所定のデータ長単位で読み出される、暗号化されたファームウエアデータであるファームウエア暗号化データと、上記乱数生成部１７ｂから出力される乱数とで排他的論理和をとることで復号し、復号された平文のファームウエアデータをＣＰＵ３５内のフラッシュＲＯＭ３８へと出力する。

【０１３７】暗号化部１８は、ストリーム暗号に対応している場合は、図１０に示すようにＳＥＥＤデータ格納部１８ａと、乱数生成部１８ｂと、排他的論理和演算部１８ｃとを備えている。

【０１３８】ＳＥＥＤデータ格納部１８ａは、乱数生成

部１８ｂの初期入力値であり共通鍵に相当するＳＥＥＤデータを格納しており、ＣＰＵコア３６からの指示に応じて格納しているＳＥＥＤデータを乱数生成部１８ｂに出力する。

【０１３９】また、ＳＥＥＤデータ格納部１８ａに格納されるＳＥＥＤデータは、固定された値があらかじめ格納されていてもよいし、ＣＰＵコア３６から適時、設定可能としてもよい。

【０１４０】なお、ＳＥＥＤデータ格納部１８ａから乱数生成部１８ｂに入力されるＳＥＥＤデータは、上述した復号部１７において、ＳＥＥＤデータ格納部１７ａから乱数生成部１７ｂに入力されるＳＥＥＤデータと同じデータである。

【０１４１】乱数生成部１８ｂは、ＳＥＥＤデータ格納部１８ａからＳＥＥＤデータが入力されたことに応じて所定のアルゴリズムで乱数を生成し、排他的論理和演算部１８ｃに出力する。

【０１４２】なお、乱数生成部１８ａで乱数生成に用いるアルゴリズムは、上述した復号部１７の乱数生成部１７ｂで乱数生成に用いるアルゴリズムと同じものである。

【０１４３】排他的論理和演算部１８ｃは、フラッシュメモリ３８から所定のデータ長単位で読み出される、平文のファームウエアデータと、上記乱数生成部１８ｂから出力される乱数とで排他的論理和をとることで暗号化し、暗号化されたファームウエア暗号化データをバッファメモリ８へと出力する。

【０１４４】ＣＰＵ３５は、ＣＰＵコア３６と、ＲＡＭ３７と、フラッシュＲＯＭ３８とを備えている。ＣＰＵ３５は、ＣＰＵ　Ｉ／Ｆ１６を介してＤＶＤデコーダ７’と接続されている。

【０１４５】ＣＰＵコア３６は、図１で示したＣＰＵコア２０と同様に、ＣＰＵ３５の中心部分で四則演算や比較判断をする論理演算装置や加算回路、レジスタなどを備えている。

【０１４６】ＲＡＭ３７は、図１で示したＲＡＭ２３と同様に、記憶内容維持のためのリフレッシュ動作が不要で高速アクセス可能なＳＲＡＭなどであり、フラッシュＲＯＭ３８内に格納されているファームウエアをアップデートする際にデータ及びアップデート用プログラムの展開領域となる。

【０１４７】フラッシュＲＯＭ３８は、例えば、データの電気的消去が可能なプログラマブルＲＯＭであるＥＥＰＲＯＭなどのいわゆるフラッシュメモリである。フラッシュＲＯＭ３８は、図１で示したフラッシュＲＯＭ２２と同様に、当該ＤＶＤ－ＲＯＭドライブの再生制限をするプログラムであるファームウエアが格納される。

【０１４８】ＤＶＤデコーダ７’の復号部１７で復号された平文のファームウエアデータは、ＣＰＵ　Ｉ／Ｆ１６を介してＣＰＵ３５内のフラッシュＲＯＭ３８に出力される。

【０１４９】なお、フラッシュＲＯＭ３８でも、図１に示したＤＶＤ－ＲＯＭドライブのＣＰＵ９内に備えられたフラッシュＲＯＭ２２と同様にＴＭＲ素子を用いたＭＲＡＭを使用することも可能である。

【０１５０】図８に示したＤＶＤ－ＲＯＭドライブでは、ＤＶＤデコーダ７’で復号された平文のファームウエアデータは、平文のままＣＰＵ３５に転送されることになる。そのため、転送される際に配線などが操作され、平文のファームウエアデータが盗み見られてしまう可能性がある。

【０１５１】したがって、平文のファームウエアが流れる箇所であるＤＶＤデコーダ７’と、ＣＰＵ３５との間の配線を、多層基板を使って内層に施すようにしたり、半導体パッケージをピンのでないボールグリッドアレイなどにするといった処理が必要となる。

【０１５２】なお、図８に示したＤＶＤ－ＲＯＭドライブのＤＶＤデコーダ７’、ＣＰＵ３５以外の機能部に関しては、図１に示したＤＶＤ－ＲＯＭドライブが備える機能部と同じであるため説明を省略する。

【０１５３】次に、図１１、図１２に示すフローチャートを用いて、フラッシュＲＯＭ３８に記憶されたファームウエアをアップデートする際の動作について説明をする。まず、図１１に示すフローチャートを用いて、アップデート（ｕｐｄａｔｅ）関数がＲＡＭ３７に読み込まれるまでの動作について説明をする。

【０１５４】ステップＳ１０１において、ＣＰＵコア３６は、ＰＣ１０から送信され、受信したコマンドがＷｒｉｔｅバッファコマンド（Write Buffer Command）であるかどうかを判定する。Ｗｒｉｔｅバッファコマンドでない場合は工程をステップＳ１０２へ進め、Ｗｒｉｔｅバッファコマンドである場合は工程をステップＳ１０３へと進める。

【０１５５】ステップＳ１０２において、ＣＰＵコア３６は、ＰＣ１０から送信されたＷｒｉｔｅバッファコマンドに、フラッシュＲＯＭ３８に記憶されているファームウエアを更新することを指示するパラメータが付加されているかどうかを検出し、付加されていない場合は工程をステップＳ１０３へと進め、付加されている場合は工程をステップＳ１０４へと進める。

【０１５６】ステップＳ１０３において、ＣＰＵコア３６は、ＰＣ１０から送信されたコマンドがＷｒｉｔｅバッファコマンドでなかったことに応じて、送信されたコマンドを実行する。また、ＣＰＵコア３６は、送信されたコマンドが、Ｗｒｉｔｅバッファコマンドであったがファームウエアを更新することを指示するパラメータが付加されていなかったことに応じて、ＰＣ１０から送信されるファームウエア以外のデータをバッファメモリ８に書き込むよう制御をする。ステップＳ１０３の工程が終了すると工程は、ステップＳ１０１へと戻る。

39

【０１５７】ＰＣ１０は、ＤＶＤ－ＲＯＭドライブにＷｒｉｔｅバッファコマンドを送信した後、更新するファームウエアをストリーム暗号化方式で暗号化したファームウエア暗号化データをバイナリーファイルとしてＤＶＤ－ＲＯＭドライブに送信する。

【０１５８】ステップＳ１０４において、ＣＰＵコア３６は、Ｗｒｉｔｅバッファコマンドを受信したことに応じて、バッファメモリ８のデータ記憶領域の所定のアドレスＮからＭ（Ｍは自然数）Ｂｙｔｅ分の領域を確保し、ＰＣ１０から送信されるバイナリーファイルを上記確保したデータ記憶領域に記憶させる。

【０１５９】ステップＳ１０５において、ＣＰＵコア３６は、転送されたバイナリーファイルのＣｈｅｃｋ　Ｓｕｍを確認する。送信されるバイナリーファイルには、Ｃｈｅｃｋ　Ｓｕｍデータが添附されている。ＣＰＵコア３６は、この添附されたＣｈｅｃｋ　Ｓｕｍデータと、送信されたされたバイナリーファイルのバイナリーデータの加算値とを比較し、一致した場合は正しくバイナリーファイルが送信されたとして工程をステップＳ１０７へと進め、一致しなかった場合はバイナリーファイルの送信が失敗したとして工程をステップＳ１０６に進める。

【０１６０】ステップＳ１０６において、ＣＰＵコア３６は、ステップＳ１０５でのＣｈｅｃｋ　Ｓｕｍデータの検証結果から正しくバイナリーファイルが送信されなかったことを、Ｃｈｅｃｋ　Ｃｏｎｄｉｔｉｏｎ　Ｓｔａｔｕｓにてコマンドを完了させることでＰＣ１０に知らせ、工程を再びステップＳ１０１へと戻す。

【０１６１】ステップＳ１０７において、ＣＰＵコア３６は、フラッシュＲＯＭ３８に格納されているフラッシュＲＯＭ３８のファームウエアを更新するアップデート関数をＲＡＭ３７にコピーし、ＲＡＭ３７でＣＰＵコア３６のプログラムを実行できる状態にする。

【０１６２】その後、ＣＰＵコア３６は、フラッシュＲＯＭ３８のファームウエア格納領域に記憶されているデータ、つまり更新前のファームウエアを消去する。なお、この消去動作は、フラッシュＲＯＭ３８がオーバーライト可能なＭＲＡＭであった場合、省略されることになる。

【０１６３】続いて、図１２に示すフローチャートを用いてアップデート（ｕｐｄａｔｅ）関数による処理動作について説明をする。

【０１６４】ステップＳ１１１において、ＣＰＵコア３６は、ＲＡＭ３７に格納されたアップデート関数の先頭アドレスにアクセスし、アップデート関数によるファームウエアのフラッシュＲＯＭ３８へのアップデートを開始する。

【０１６５】ステップＳ１１２において、ＣＰＵコア３６は、図示しない割り込み制御回路を制御して全ての割り込みプログラムの実行と、例外処理の実行を禁止する。

40

【０１６６】ステップＳ１１３において、ＣＰＵコア３６は、フラッシュＲＯＭ３８への書き込みタイミングを制御する図示しない書き込みタイミング制御用タイマーを起動する。以下、フラッシュＲＯＭ３８へデータを書き込む際は、書き込みタイミング制御用タイマーのタイミング制御に基づいて実行される。

【０１６７】ステップＳ１１４において、ＣＰＵコア３６は、ファームウエア暗号化データのバイナリファイルが記憶されているバッファメモリ８のアドレス番号Ｎと、ファームウエアを記憶させるフラッシュＲＯＭ３８のアドレス番号０にアクセスをする。

【０１６８】ステップＳ１１５において、ＣＰＵコア３６は、バッファメモリ８のアドレス番号Ｎから復号に都合のよい単位ごと（例えば、１Ｂｙｔｅのデータ）に読み出し、復号部１７で復号処理をして平文にする。ＣＰＵコア３６は、復号され平文であるファームウエアデータを、当該ＣＰＵコア３６内のレジスタ又はＲＡＭ３７に格納する。

【０１６９】さらに、ＣＰＵコア３６は、当該ＣＰＵコア３６内のレジスタ又はＲＡＭ３７に格納されたファームウエアデータを読み出し、フラッシュＲＯＭ３８のアドレス番号０から書き込む。

【０１７０】ステップＳ１１６において、ＣＰＵコア３６は、フラッシュＲＯＭ３８にファームウエアデータが全て書き込まれたかどうかを判断する。ＣＰＵコア３６は、アドレス番号がＭでない場合には工程をステップＳ１１７へと進め、アドレス番号がＭとなったら工程をステップＳ１１８に進める。

【０１７１】ステップＳ１１７において、ＣＰＵコア３６は、バッファメモリ８のアドレス番号及びフラッシュＲＯＭ３８のアドレス番号を１Ｂｙｔｅ増やしたアドレス番号へアクセスをする。この工程が終了するとステップＳ１１５へと戻り、バッファメモリ８のアクセスしたアドレス番号からファームウエア暗号データを読み出し、復号処理をして復号された平文のファームウエアデータをフラッシュＲＯＭ３８のアクセスしたアドレス番号に書き込む。

【０１７２】ステップＳ１１８において、ＣＰＵコア３６は、フラッシュＲＯＭ３８への書き込みタイミングを制御する図示しない書き込みタイミング制御用タイマーを停止させる。

【０１７３】ステップＳ１１９において、ステップＳ１１６で、フラッシュＲＯＭ３８に記憶されたファームウエアデータの最終アドレス番号がＭであると判定され、ステップＳ１１８で、図示しない書き込みタイミング制御用タイマーが停止されたことで、ファームウエアのフラッシュＲＯＭ３８へのアップデートが完了する。

【０１７４】このようにして、本発明を適用した図８に示すＤＶＤ－ＲＯＭドライブでは、フラッシュＲＯＭ３

８に格納されているファームウエアをアップデートする際、ＰＣ１０でストリーム暗号方式で暗号化されたファームウエア暗号化データを、ＤＶＤデコーダ７’内の復号部１７で復号し、ＣＰＵ３５内のフラッシュＲＯＭ３８に書き込む。

【０１７５】ＤＶＤデコーダ７’と、ＣＰＵ３５とのやり取りでは、平文のファームウエアデータが転送されることになるが、配線処理や半導体パッケージの端子部分が露出しないといった実装レベルの工夫をすることで、ファームウエアデータの漏洩を防ぐことができる。

【０１７６】次に、図１３に示すフローチャートを用いて、フラッシュＲＯＭ３８にファームウエアをアップデートした結果をＰＣ１０で検証する際の処理動作について説明をする。

【０１７７】ステップＳ１２１において、ＣＰＵコア３６は、ＰＣ１０から送信され、受信したコマンドがＲｅａｄバッファコマンド（Read Buffer Command）であるかどうかを判定する。Ｒｅａｄバッファコマンドでない場合は工程をステップＳ１２３へ進め、Ｒｅａｄバッファコマンドである場合は工程をステップＳ１２２へと進める。

【０１７８】ステップＳ１２２において、ＣＰＵコア３６は、ＰＣ１０から送信されたＲｅａｄバッファコマンドに、フラッシュＲＯＭ３８に記憶されているファームウエアを読み出すことを指示するパラメータが付加されているかどうかを検出し、付加されていない場合は工程をステップＳ１２３へと進め、付加されている場合は工程をステップＳ１２４へと進める。

【０１７９】ステップＳ１２３において、ＣＰＵコア３６は、ＰＣ１０から送信されたコマンドがＲｅａｄバッファコマンドでなかったことに応じて、送信されたコマンドを実行する。また、ＣＰＵコア３６は、送信されたコマンドが、Ｒｅａｄバッファコマンドであったがファームウエアを更新することを指示するパラメータが付加されていなかったことに応じて、ファームウエア以外のデータをバッファメモリ８に読み出すよう制御をする。ステップＳ１２３が終了すると工程は終了する。

【０１８０】ＰＣ１０は、ＤＶＤ－ＲＯＭドライブにＲｅａｄバッファコマンドを送信した後、更新するファームウエアをストリーム暗号化方式で暗号化したファームウエア暗号化データをバイナリーファイルとしてＤＶＤ－ＲＯＭドライブに送信する。

【０１８１】ステップＳ１２４において、ＣＰＵコア３６は、バッファメモリ８のアドレス番号Ｎと、ファームウエアが記憶されているフラッシュＲＯＭ３８のアドレス番号０にアクセスをする。

【０１８２】ステップＳ１２５において、ＣＰＵコア３６は、フラッシュＲＯＭ３８のアドレス番号０から復号に都合のよい単位ごと（例えば、１Ｂｙｔｅのデータ）に読み出し、当該ＣＰＵコア３６内のレジスタ又はＲＡＭ３７に格納する。

【０１８３】さらに、ＣＰＵコア３６は、当該ＣＰＵコア３６内のレジスタ又はＲＡＭ３７に格納された平文であるファームウエアデータを読み出し、ＤＶＤデコーダ７’の暗号化部１８で暗号化処理をしてファームウエア暗号化データにする。ＣＰＵコア３６は、暗号化されたファームウエア暗号化データをバッファメモリ８のアドレス番号Ｎから書き込む。

【０１８４】ステップＳ１２６において、ＣＰＵコア３６は、フラッシュＲＯＭ３８からファームウエアデータが全て読み出されたかどうかを判断する。ＣＰＵコア３６は、アドレス番号がＭでない場合には工程をステップＳ１２７へと進め、アドレス番号がＭとなったら工程をステップＳ１２８に進める。

【０１８５】ステップＳ１２７において、ＣＰＵコア３６は、バッファメモリ８のアドレス番号及びフラッシュＲＯＭ３８のアドレス番号を１Ｂｙｔｅ増やしたアドレス番号へアクセスをする。この工程が終了するとステップＳ１２５へと戻り、フラッシュＲＯＭ３８のアクセスしたアドレス番号からファームウエアデータを読み出し、暗号化処理をして暗号化されたファームウエア暗号化データをバッファメモリ８のアクセスしたアドレス番号に書き込む。

【０１８６】ステップＳ１２８において、フラッシュＲＯＭ３８に格納されているファームウエアデータが全て読み出され、暗号化されてバッファメモリ８に格納されたことに応じて、ＣＰＵコア３６は、バッファメモリ８に格納されているファームウエア暗号化データをＰＣ１０へと転送する。

【０１８７】転送されたファームウエア暗号化データは、ＰＣ１０にて暗号化されたまま元データと比較され一致が確認される。

【０１８８】このようにして、ＰＣ１０は、ＤＶＤ－ＲＯＭドライブのフラッシュＲＯＭ３８にファームウエアが確実に更新されているかどうかを検証することができる。

【０１８９】ＤＶＤデコーダ７’と、ＣＰＵ３５とのやり取りでは、平文のファームウエアデータが転送されることになるが、配線処理や半導体パッケージの端子部分が露出しないといった実装レベルの工夫をすることで、ファームウエアデータの漏洩を防ぐことができる。

【０１９０】ところで、一般に、ＰＣ（Personal Computer）などにおいて実行されるプログラムは、ＨＤ（Hard Disk）などの補助記憶装置に記憶されており、ＰＣの電源起動時にＲＡＭ（Random Access Memory）などの主記憶装置にロードされる。ＣＰＵは、主記憶装置にロードされたプログラムを読み込んで、プログラムの実行をする。

【０１９１】このように、ＣＰＵが実行するプログラムを主記憶装置にロードするには、ＣＰＵコア内に常駐、

又は、上記HDから最初に読み込まれるIPL（Initial Program Loader）によって行われる。

【0192】一方、第1の実施の形態として図1を用いて説明したDVD-ROMドライブ、及び第2の実施の形態として図8を用いて説明したDVD-ROMドライブでは、DVDデコーダにCPUを備えている場合がある。このように、DVDデコーダに備えられたCPUも上述したPCと同様に外部の記憶部に格納されているプログラムをRAMに読み出し、RAMに読み出したプログラムを実行させることでDVDデコードなどの所定の処理を行うことになる。

【0193】したがって、外部の記憶部に格納されているプログラムは、DVDデコーダ内のRAMに読み出される際、盗み見られ、プログラムの解析や改竄といった行為がなされてしまう可能性があるため暗号化して格納されている必要がある。

【0194】なお、以下の説明においては、DVDデコーダが備えるCPUが実行するプログラムをマイクロプログラムと呼び、そのデータをマイクロプログラムデータと呼ぶ。また、マイクロプログラムデータが暗号化されたものは暗号化マイクロプログラムデータと呼ぶ。

【0195】図14に第3の実施の形態として示すDVD-ROMドライブでは、DVDデコーダとして、図1で示したDVDデコーダ7に、内部CPUコア41と、SRAM42と、復号部43とを付加したDVDデコーダ7"を備えている。内部CPUコア41、SRAM42、復号部43は、メモリ制御部14、CPU I/F16と内部バスで接続されている。また、図14に示したDVD-ROMドライブでは、外部CPU45と、DVDデコーダ7"に読み込まれる暗号化されたマイクロプログラムデータ（暗号化マイクロプログラムデータ）が格納されたフラッシュROM46とを備えている。

【0196】内部CPUコア41は、DVDデコーダ7"制御用のマイクロコントローラである。内部CPUコア41は、自身が実行するマイクロプログラムをSRAM42に読み込ませるためのプログラムであるIPLを格納している。DVD-ROMドライブに電源が投入されるとIPLが起動することになる。

【0197】SRAM42は、内部CPUコア41で実行するマイクロプログラムデータを格納する内部CPUコア41に対する主記憶装置である。SRAM42には、IPLによってフラッシュROM46から読み出された暗号化マイクロプログラムデータが復号部43で復号されて格納される。

【0198】復号部43は、フラッシROM46に格納されている暗号化されたマイクロプログラムデータ（暗号化マイクロプログラムデータ）を復号してSRAM42のプログラム領域へ転送するための復号回路である。復号部43は、共通鍵暗号（ブロック暗号、ストリーム暗号）化方式で暗号化されたマイクロプログラムデータ

（暗号化マイクロプログラムデータ）を復号する。

【0199】復号部43は、ストリーム暗号に対応している場合は、図15に示すようにSEEDデータ格納部43aと、乱数生成部43bと、排他的論理和演算部43cとを備えている。

【0200】SEEDデータ格納部43aは、乱数生成部43bの初期入力値であり共通鍵に相当するSEEDデータを格納しており、内部CPUコア41からの指示に応じて格納しているSEEDデータを乱数生成部43bに出力する。

【0201】また、SEEDデータ格納部43aに格納されるSEEDデータは、固定された値があらかじめ格納されていてもよいし、内部CPUコア41から適時、設定可能としてもよい。

【0202】乱数生成部43bは、SEEDデータ格納部43aからSEEDデータが入力されたことに応じて所定のアルゴリズムで乱数を生成し、排他的論理和演算部43cに出力する。

【0203】排他的論理和演算部43cは、フラッシュROM46から所定のデータ長単位で読み出される、暗号化されたマイクロプログラムデータである暗号化マイクロプログラムデータと、上記乱数生成部43bから出力される乱数とで排他的論理和をとることで復号し、復号された平文のマイクロプログラムデータをDVDデコーダ7"内のSRAM42へと出力する。

【0204】また、DVDデコーダ7"のCPU I/F16は、当該DVDデコーダ7"内のSRAM42に格納されているマイクロプログラムデータ、復号部43のSEEDデータ格納部43aに格納されているSEEDデータ、乱数生成部43bの乱数生成アルゴリズムをユーザレベルでは参照できないような保護機能を備えている。これにより、復号された平文のマイクロプログラムデータ、及び、暗号化マイクロプログラムデータを復号するための復号機能を取り出すことを制限することができる。

【0205】外部CPU45は、DVD-ROMドライブを統括的に制御する制御部であり、四則演算や比較判断をする論理演算装置や加算回路、レジスタなどを備えている。

【0206】フラッシュROM46は、例えば、データの電気的消去が可能なプログラマブルROMであるEEPROMなどのいわゆるフラッシュメモリである。フラッシュROM46は、内部CPUコア41の実行プログラムが暗号化さた暗号化マイクロプログラムデータを格納している。

【0207】続いて、図16に示すフローチャートを用いて、図14に示すDVD-ROMドライブの起動時の動作について説明をする。

【0208】ステップS131において、電源投入リセットにより、内部CPUコア41内に常駐するIPLが

45

起動する。ＩＰＬが起動すると同時に、復号部４３では、ＳＥＥＤデータを乱数生成部４３ｂが取り込むことで初期化が行われる。

【０２０９】ステップＳ１３２において、内部ＣＰＵコア４１で実行されるＩＰＬによって、フラッシュＲＯＭ４６の先頭アドレスから、当該フラッシュＲＯＭ４６に格納されている暗号化マイクロプログラムデータの読み出しが開始される。読み出された暗号化マイクロプログラムデータは、復号部４３に入力され乱数生成部４３ａからの出力データと排他的論理和をとって平文であるマイクロプログラムデータに復号される。復号されたマイクロプログラムデータは、ＳＲＡＭ４２に書き込まれる。

【０２１０】ステップＳ１３３において、内部ＣＰＵコア４１で実行されるＩＰＬによって、フラッシュＲＯＭ４６内に格納されている暗号化マイクロプログラムデータが所定の量だけ読み出されたかどうか判定される。所定量の暗号化マイクロプログラムデータが読み出された場合は、工程をステップＳ１３４へと進め、所定量の暗号化マイクロプログラムデータが読み出されていない場合は、フラッシュＲＯＭ４６からの読み出し、復号部４３での復号、ＳＲＡＭ４２への書き込みが実行される。

【０２１１】ステップＳ１３４において、内部ＣＰＵコア４１で実行されるＩＰＬによって、フラッシュＲＯＭ４６からの読み出しが完了すると、内部ＣＰＵコア４１は、内蔵するプログラムカウンタの値をＳＲＡＭ４２の先頭アドレスとし、ＳＲＡＭ４２内に書き込まれた平文であるマイクロプログラムデータを実行する。

【０２１２】このようにして、フラッシュＲＯＭ４６に格納されている暗号化マイクロプログラムデータは、図１４に示すＤＶＤ－ＲＯＭドライブが起動するとともにＩＰＬによって読み出され、ＤＶＤデコーダ７”内で復号され、ＳＲＡＭ４２に書き込まれる。したがって、ＤＶＤデコーダ７”内部ＣＰＵコア４１が実行するマイクロプログラムは、当該ＤＶＤデコーダ７”内で暗号が復号されるため、プログラムの解析や改竄を防止することができる。

【０２１３】上述したように、ＤＶＤ－ＲＯＭドライブのファームウエアを更新する際、暗号化してＰＣ１０からＤＶＤ－ＲＯＭドライブへ転送し、図１に示したＣＰＵ９内、又は、図８に示したＤＶＤデコーダ７’内で復号してＣＰＵ内のフラッシュＲＯＭに更新することで、更新時の解析や改竄を防止することができる。また、図１４に示したＤＶＤ－ＲＯＭドライブのように起動時にロードするプログラムも暗号化したまま復号する回路内に読み出し、当該回路内で暗号を復号することでロード時のプログラムの解析や改竄を防止することができる。

【０２１４】なお、図１４を用いて説明したＤＶＤ－ＲＯＭドライブにおいて、ＳＲＡＭ４２へ格納するマイクロプログラムは、ＤＶＤデコーダ７”にバスで接続されたフラッシュＲＯＭ４６から供給されるとしているが、例えば、読み出し専用ＲＯＭ、ディスク状記録媒体、リムーバル半導体メモリなど、どんなものであってもかまわない。

46

【０２１５】また、図１４を用いて説明したＤＶＤ－ＲＯＭドライブでは、フラッシュＲＯＭ４６から復号部４３を経由したＳＲＡＭ４２へのマイクロプログラムの読み出し処理を、ＤＶＤデコーダ７”に内蔵されている内部ＣＰＵコア４１が備えるＩＰＬによって実行していたが、ＤＶＤデコーダ７”の外部にあるＣＰＵ、例えば、外部ＣＰＵ４５などの制御によって実施するようにしてもよい。

【０２１６】しかし、上述したように暗号化されたプログラムの復号後のデータ漏洩を防止できたとしても、暗号化されたままプログラムが改竄されるということも考えられる。

【０２１７】例えば、図１に示したＤＶＤ－ＲＯＭドライブで、ファームウエアが暗号化されたまま改竄されると、フラッシュＲＯＭ２２には、そのまま改竄されたデータが格納されてしまうことになり、コンテンツの違法複製、ドライブの動作不良などを引き起こしてしまう可能性がある。

【０２１８】そこで、更新するプログラム本体にプログラムが改竄されたことを検証する検証プログラムを添付してＤＶＤ－ＲＯＭドライブに送信するといった手法が考えられる。更新するプログラム本体にこの検証プログラムを添付すると、ＤＶＤ－ＲＯＭドライブで更新されたプログラムを実行すると、まずプログラム本体に添附した検証プログラムが起動し、更新されたプログラムが改竄されているか否かを検証することができる。

【０２１９】図１７、図１８、図１９に示すフローチャートを用いて、上述した暗号化データの改竄を防止して、プログラムの更新をする動作について説明をする。なお、説明のためプログラムを更新するドライブとして図８に示したＤＶＤ－ＲＯＭドライブを用いる。

【０２２０】まず、図１７に示したフローチャートを用いて検証プログラムを添附したプログラム本体をＤＶＤ－ＲＯＭドライブに送信するまでの動作について説明をする。

【０２２１】ステップＳ１４１において、例えば、ドライブ製造会社などによってＤＶＤ－ＲＯＭドライブに送信するプログラムが作成される。作成されるプログラム本体には、上述したプログラムの改竄を検証するための検証プログラムが添附されている。

【０２２２】ステップＳ１４２において、ドライブ製造会社は、配布するプログラムから検証データを生成し、図２０に示すように生成した検証データをプログラムに付加する。

【０２２３】この検証データは、ハッシュ関数を用いてプログラム本体を演算することで得られるハッシュ値で

ある。例えば、図２１に示すようにハッシュ関数として、米国商務省に所属する標準化機関ＮＩＳＴによって定められたハッシュアルゴリズムであるＳＨＡ（Secure Hash Algorithm）をさらに改良したＳＨＡ－１を使用することができる。ＳＨＡ－１は、2^{64}ビット未満のデータ長から１６０ビット長のハッシュ値（検証データ）を生成するアルゴリズムである。

【０２２４】ステップＳ１４３において、ドライブ製造会社は、検証データが付加されたプログラムを、図２２に示すように検証データも含めて暗号化する。

【０２２５】ステップＳ１４４において、ドライブ製造会社は、暗号化されたプログラムからＣｈｅｃｋ　Ｓｕｍデータを算出し、図２３に示すようにＣｈｅｃｋ　Ｓｕｍデータを付加する。付加するデータは、Ｃｈｅｃｋ　Ｓｕｍデータに代えて、再びハッシュ関数により求めたハッシュ値であってもよい。Ｃｈｅｃｋ　Ｓｕｍデータが付加されることでプログラムは、送信可能なデータとなる。

【０２２６】送信可能なデータは、例えば、ＲＯＭメディアなどを使って、ユーザ（ＰＣ１０）に配布される。

【０２２７】ステップＳ１４５において、ＰＣ１０は、ＤＶＤ－ＲＯＭドライブに送信可能となったデータ（プログラム）を送信する。

【０２２８】次に、図１８に示すフローチャートを用いて、ＰＣ１０から送信された暗号化データの改竄防止措置がなされたプログラムを受信するＤＶＤ－ＲＯＭドライブの動作について説明をする。

【０２２９】ステップＳ１５１において、ＤＶＤ－ＲＯＭドライブは、ＰＣ１０からＷｒｉｔｅバッファコマンドとともに送信されるプログラムを受信すると、プログラムに添付されたＣｈｅｃｋ　Ｓｕｍデータと、送信されたプログラム暗号化データの加算値とを比較する。一致しなかった場合は工程をステップＳ１５２へと進め、一致した場合は工程をステップＳ１５３へと進める。

【０２３０】ステップＳ１５２において、Ｃｈｅｃｋ　Ｓｕｍデータの比較結果から正しくプログラム暗号化データが送信されなかったことをＣｈｅｃｋ　Ｃｏｎｄｉｔｉｏｎ　Ｓｔａｔｕｓにてコマンド完了することでＰＣ１０に知らせ、工程を再びステップＳ１５１へと戻す。

【０２３１】ステップＳ１５３において、復号部１７は、プログラム暗号化データを復号する。復号されたデータには検証データが付加されており、プログラム本体には検証プログラムが記述されている。

【０２３２】ステップＳ１５４において、復号されたプログラムデータは、フラッシュＲＯＭ３８に格納される。

【０２３３】ステップＳ１５５において、フラッシュＲＯＭ３８に格納されたプログラムが起動すると、まず始めに検証プログラムが動作する。

【０２３４】次に、図１９に示すフローチャートを用いて、検証プログラムの動作を説明する。

【０２３５】ステップＳ１６１において、起動した検証プログラムは、プログラム本体のハッシュ値をハッシュ関数により計算する。

【０２３６】ステップＳ１６２において、検証プログラムは、ハッシュ値が計算されるとプログラム本体に添附された検証データと、計算されたハッシュ値と比較し、一致した場合は工程をステップＳ１６３へと進め、一致しなかった場合は工程をステップＳ１６４へと進める。

【０２３７】ステップＳ１６３において、ＤＶＤ－ＲＯＭドライブは、添附された検証データと、計算したハッシュ値とが一致し、フラッシュＲＯＭ３８に格納されたプログラムが改竄されていないプログラムであると判定されたことに応じて、フラッシュＲＯＭ３８に格納されたプログラム本体を実行する。

【０２３８】ステップＳ１６４において、ＤＶＤ－ＲＯＭドライブは、添附された検証データと、計算したハッシュ値とが一致せず、フラッシュＲＯＭ３８に格納されたファームウエアが改竄されたプログラムであると判定されたことに応じて、ＮｏｔＲｅａｄｙ状態となり、何も動作しない安定な状態となる。

【０２３９】このようにして、送信するプログラム本体に、ハッシュ関数によって算出された検証データを付加して送信することで、ＤＶＤ－ＲＯＭドライブは、暗号化データそのものが改竄された場合であっても改竄されたことを検証することができる。

【０２４０】なお、上述した本発明の第１の実施の形態、第２の実施の形態として示すＤＶＤ－ＲＯＭドライブでは、ファームウエアを更新する際、更新するファームウエアをＰＣ１０から送信されるようにしているが、ファームウエアは、例えば、当該ＤＶＤ－ＲＯＭドライブで再生可能なＤＶＤ－ＲＯＭ１に記録されていてもよい。ＤＶＤ－ＲＯＭ１にファームウエア暗号化データをファイルとして記憶することで、ＤＶＤ－ＲＯＭドライブは、このＤＶＤ－ＲＯＭ１を再生することによって更新するファームウエアを取得することができる。

【０２４１】同様に、本発明の第３の実施の形態として示すＤＶＤ－ＲＯＭドライブでは、暗号化マイクロプログラムデータをファイルとして記録したＤＶＤ－ＲＯＭ１を再生することによってマイクロプログラムをロードするようにしてもよい。

【０２４２】また、このＤＶＤ－ＲＯＭ１には、本発明の第１の実施の形態として示したＤＶＤ－ＲＯＭドライブのブートＲＯＭ２１に書き込まれているファームウエア更新時に起動するプログラムが書き込まれていてもよく、上述のようにＤＶＤ－ＲＯＭドライブはＤＶＤ－ＲＯＭ１を再生することでファームウエアを更新させることができる。

【０２４３】同様に、ＤＶＤ－ＲＯＭ１には、本発明の

第２の実施の形態として示したＤＶＤ－ＲＯＭドライブでファームウエア更新時に起動するプログラムが書き込まれいてもよく、上述のようにＤＶＤ－ＲＯＭドライブはＤＶＤ－ＲＯＭ１を再生することでファームウエアを更新させることができる。

【０２４４】同様に、ＤＶＤ－ＲＯＭ１には、本発明の第３の実施の形態として示したＤＶＤ－ＲＯＭドライブでマイクロプログラムをロードする時に起動するプログラムが書き込まれいてもよく、上述のようにＤＶＤ－ＲＯＭドライブはＤＶＤ－ＲＯＭ１を再生することでマイクロプログラムをロードさせることができる。

【０２４５】また、本発明の第１の実施の形態及び第２の実施の形態として示したＤＶＤ－ＲＯＭドライブにおいて、メモリースティック（登録商標）などのリムーバル半導体メモリーに対応した半導体メモリー用スロットを設け、上述したＤＶＤ－ＲＯＭ１の代わりにファームウエア暗号化データを上記リムーバル半導体メモリーへ記録してファームウエアを更新するようにしてもよい。

【０２４６】同様に、本発明の第３の実施の形態として示したＤＶＤ－ＲＯＭドライブでも、暗号化マイクロプログラムデータを上記リムーバル半導体メモリへ記録してマイクロプログラムをロードするようにしてもよい。

【０２４７】さらにまた、上述のように本発明の第１の実施の形態、第２の実施の形態及び第３の実施の形態としてＤＶＤ－ＲＯＭドライブを適用しているが、本発明はこれに限定されるものではなく、ＣＤ－ＲＯＭ、データが記録されたＣＤ－Ｒ、ＣＤ－ＲＷ、ＤＶＤ－ＲＡＭ、ＤＶＤ－Ｒ／ＲＷ、ＤＶＤ＋Ｒ／ＲＷを記録再生可能なディスク装置全般に適用することが可能である。

【０２４８】また、本発明を適用した第１の実施の形態、第２の実施の形態及び第３の実施の形態としてＤＶＤ－ＲＯＭドライブを用いたが、本発明はこれに限定されるものではなく、何らかのセキュリティが必要な処理装置全般に適用可能である。

【０２４９】また、ファームウエア又はマイクロプログラムを暗号化し、復号する手法として共通鍵を用いた暗号化手法を用いているが、本発明はこれに限定されるものではなく、公開鍵方式やそれ以外の暗号化アルゴリズムを適用してもかまわない。

【０２５０】さらにまた、本発明を適用した第１の実施の形態、第２の実施の形態及び第３の実施の形態として示したＤＶＤ－ＲＯＭドライブでは、ファームウエアや、マイクロプログラムを対象としていたが、当該ＤＶＤ－ＲＯＭドライブ内の書き換え可能なレジスタ・メモリの設定値というようにデータを対象とし、更新又は設定などをしてもよい。

【０２５１】

【発明の効果】以上の説明からも明らかなように、本発明の情報処理装置は、復号手段で、暗号化プログラムデータを所定の復号鍵を用いてプログラムに復号し、復号

したプログラムを記憶手段に記憶させ、記憶したプログラムを読み出し、読み出したプログラムに基づいて制御手段で当該情報処理装置の所定の動作を制御することで、プログラムロード時における外部へのプログラムデータの漏洩を阻止することができるため、プログラムをロードする際に漏洩したプログラムデータを用いた違法行為を防止することが可能となる。

【０２５２】例えば、ＤＶＤ－ＲＯＭドライブのファームウエアを更新することでファームウエアデータが漏洩した場合に生ずるリージョナルコード（RC：Regional Code）による再生制限の無効化や、ＤＶＤ－ＲＯＭの違法コピー及び違法コピーＤＶＤ－ＲＯＭの再生制限の無効化といった違法行為を防止することが可能となる。

【０２５３】また、以上の説明からも明らかなように、本発明のプログラムロード方法は、復号ステップで、暗号化プログラムデータを所定の復号鍵を用いてプログラムに復号し、復号したプログラムを記憶手段に記憶させ、記憶したプログラムを読み出し、読み出したプログラムに基づいて制御ステップで当該情報処理装置の所定の動作を制御することで、プログラムロード時における外部へのプログラムデータの漏洩を阻止することができるため、プログラムをロードする際に漏洩したプログラムデータを用いた違法行為を防止することが可能となる。

【０２５４】例えば、ＤＶＤ－ＲＯＭドライブのファームウエアを更新することでファームウエアデータが漏洩した場合に生ずるリージョナルコード（RC：Regional Code）による再生制限の無効化や、ＤＶＤ－ＲＯＭの違法コピー及び違法コピーＤＶＤ－ＲＯＭの再生制限の無効化といった違法行為を防止することが可能となる。

【０２５５】また、以上の説明からも明らかなように、本発明の記録媒体は、復号ステップで、暗号化プログラムデータを所定の復号鍵を用いてプログラムに復号し、復号したプログラムを記憶手段に記憶させ、記憶したプログラムを読み出し、読み出したプログラムに基づいて制御ステップで当該情報処理装置の所定の動作を制御することを特徴とするプログラムを記録することで、プログラムロード時における外部へのプログラムデータの漏洩を阻止することができるため、プログラムをロードする際に漏洩したプログラムデータを用いた違法行為を防止することが可能となる。

【０２５６】例えば、ＤＶＤ－ＲＯＭドライブのファームウエアを更新することでファームウエアデータが漏洩した場合に生ずるリージョナルコード（RC：Regional Code）による再生制限の無効化や、ＤＶＤ－ＲＯＭの違法コピー及び違法コピーＤＶＤ－ＲＯＭの再生制限の無効化といった違法行為を防止することが可能となる。

【０２５７】以上の説明からも明らかなように、本発明の情報処理装置は、プログラム更新要求に応じて、制御部内の復号手段で、第２のプログラムを所定の暗号化鍵

で暗号化した暗号化プログラムデータを所定の復号鍵を用いて第２のプログラムに復号し、プログラム書き込み手段で復号した第２のプログラムを記憶手段に書き込んで第１のプログラムを更新し、さらに、取り出し制限手段で復号手段で復号された第２のプログラム及び記憶手段に書き込まれた第２のプログラムの外部装置からの取り出しを制限することで、プログラム更新時における外部へのプログラムデータの漏洩を阻止することができるため、プログラムを更新する際に漏洩したプログラムデータを用いた違法行為を防止することが可能となる。

【０２５８】例えば、ＤＶＤ－ＲＯＭドライブのファームウエアを更新することでファームウエアデータが漏洩した場合に生ずるリージョナルコード（RC：Regional Code）による再生制限の無効化や、ＤＶＤ－ＲＯＭの違法コピー及び違法コピーＤＶＤ－ＲＯＭの再生制限の無効化といった違法行為を防止することが可能となる。

【０２５９】また、本発明の情報処理装置は、制御部のアーキテクチャを新たに構築する必要がないため、安価に製造することができる。

【０２６０】さらに、本発明の情報処理装置は、プログラムの更新時にだけ制御部内で暗号復号処理をするので、通常時における制御部の処理動作を低下させることがない。

【０２６１】また、以上の説明からも明らかなように、本発明のプログラム更新方法は、プログラム更新要求に応じて、復号ステップで、第２のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを所定の復号鍵を用いて第２のプログラムに復号し、プログラム書き込みステップで復号した第２のプログラムを記憶手段に書き込んで第１のプログラムを更新し、さらに、取り出し制限ステップで復号ステップで復号された第２のプログラム及び記憶手段に書き込まれた第２のプログラムの外部装置からの取り出しを制限することで、プログラム更新時における外部へのプログラムデータの漏洩を阻止することができるため、プログラムを更新する際に漏洩したプログラムデータを用いた違法行為を防止することが可能となる。

【０２６２】例えば、ＤＶＤ－ＲＯＭドライブのファームウエアを更新することでファームウエアデータが漏洩した場合に生ずるリージョナルコード（RC：Regional Code）による再生制限の無効化や、ＤＶＤ－ＲＯＭの違法コピー及び違法コピーＤＶＤ－ＲＯＭの再生制限の無効化といった違法行為を防止することが可能となる。

【０２６３】さらに、本発明のプログラム更新方法は、第１のプログラムの更新時にだけ制御部内で暗号復号処理をするので、通常時における制御部の処理動作を低下させることがない。

【０２６４】また、以上の説明からも明らかなように、本発明の記録媒体は、プログラム更新要求に応じて、復号ステップで、第２のプログラムを所定の暗号化鍵で暗

号化した暗号化プログラムデータを所定の復号鍵を用いて第２のプログラムに復号し、プログラム書き込みステップで復号した第２のプログラムを記憶手段に書き込んで第１のプログラムを更新し、さらに、取り出し制限ステップで復号ステップで復号された第２のプログラム及び記憶手段に書き込まれた第２のプログラムの外部装置からの取り出しを制限することでことを特徴とするプログラムを記録することで、プログラム更新時における外部へのプログラムデータの漏洩を阻止することができるため、プログラムを更新する際に漏洩したプログラムデータを用いた違法行為を防止することが可能となる。

【０２６５】例えば、ＤＶＤ－ＲＯＭドライブのファームウエアを更新することでファームウエアデータが漏洩した場合に生ずるリージョナルコード（RC：Regional Code）による再生制限の無効化や、ＤＶＤ－ＲＯＭの違法コピー及び違法コピーＤＶＤ－ＲＯＭの再生制限の無効化といった違法行為を防止することが可能となる。

【０２６６】さらに、本発明の記録媒体に記録されたプログラムは、第１のプログラムの更新時にだけ制御部内で暗号復号処理をするので、通常時における制御部の処理動作を低下させることがない。

【０２６７】また、以上の説明からも明らかなように、本発明の回路素子は、プログラム更新要求に応じて、集積化された復号手段で第２のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを所定の復号鍵を用いて第２のプログラムに復号し、プログラム書き込み手段で復号した第２のプログラムを記憶手段に書き込んで第１のプログラムを更新し、さらに、取り出し制限手段で復号手段で復号された第２のプログラム及び記憶手段に書き込まれた第２のプログラムの外部装置からの取り出しを制限することで、プログラム更新時における外部へのプログラムデータの漏洩を阻止することができるため、プログラムを更新する際に漏洩したプログラムデータを用いた違法行為を防止することが可能となる。

【０２６８】例えば、ＤＶＤ－ＲＯＭドライブのファームウエアを更新することでファームウエアデータが漏洩した場合に生ずるリージョナルコード（RC：Regional Code）による再生制限の無効化や、ＤＶＤ－ＲＯＭの違法コピー及び違法コピーＤＶＤ－ＲＯＭの再生制限の無効化といった違法行為を防止することが可能となる。

【０２６９】さらに、本発明の回路素子は、第１のプログラムの更新時にだけ当該回路素子内で暗号復号処理をするので、通常時における当該回路素子の処理動作を低下させることがない。

【０２７０】以上の説明からも明らかなように、本発明の情報処理装置は、プログラム更新要求に応じて、データ処理部内の復号手段で、第２のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを所定の復号鍵を用いて第２のプログラムに復号して制御部に送信し、制御部のプログラム書き込み手段で復号した第２の

プログラムを制御部内の記憶手段に書き込んで第１のプログラムを更新することで、プログラム更新時における外部へのプログラムデータの漏洩を少なくできるため、プログラムを更新する際に漏洩したプログラムデータを用いた違法行為を防止することが可能となる。

【０２７１】例えば、ＤＶＤ－ＲＯＭドライブのファームウエアを更新することでファームウエアデータが漏洩した場合に生ずるリージョナルコード（RC：Regional Code）による再生制限の無効化や、ＤＶＤ－ＲＯＭの違法コピー及び違法コピーＤＶＤ－ＲＯＭの再生制限の無効化といった違法行為を防止することが可能となる。

【０２７２】また、以上の説明からも明らかなように、本発明のプログラム更新方法は、プログラム更新要求に応じて、復号ステップで、第２のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを所定の復号鍵を用いて第２のプログラムに復号して制御部に送信し、プログラム書き込みステップで復号した第２のプログラムを制御部内の記憶手段に書き込んで第１のプログラムを更新することで、プログラム更新時における外部へのプログラムデータの漏洩を少なくできるため、プログラムを更新する際に漏洩したプログラムデータを用いた違法行為を防止することが可能となる。

【０２７３】例えば、ＤＶＤ－ＲＯＭドライブのファームウエアを更新することでファームウエアデータが漏洩した場合に生ずるリージョナルコード（RC：Regional Code）による再生制限の無効化や、ＤＶＤ－ＲＯＭの違法コピー及び違法コピーＤＶＤ－ＲＯＭの再生制限の無効化といった違法行為を防止することが可能となる。

【０２７４】また、以上の説明からも明らかなように、本発明の記録媒体は、プログラム更新要求に応じて、復号ステップで、第２のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを所定の復号鍵を用いて第２のプログラムに復号して制御部に送信し、プログラム書き込みステップで復号した第２のプログラムを制御部内の記憶手段に書き込んで第１のプログラムを更新することを特徴とするプログラムを記録することで、プログラム更新時における外部へのプログラムデータの漏洩を少なくできるため、プログラムを更新する際に漏洩したプログラムデータを用いた違法行為を防止することが可能となる。

【０２７５】例えば、ＤＶＤ－ＲＯＭドライブのファームウエアを更新することでファームウエアデータが漏洩した場合に生ずるリージョナルコード（RC：Regional Code）による再生制限の無効化や、ＤＶＤ－ＲＯＭの違法コピー及び違法コピーＤＶＤ－ＲＯＭの再生制限の無効化といった違法行為を防止することが可能となる。

【０２７６】以上の説明からも明らかなように、本発明の情報処理装置は、データ処理部内の復号手段で、所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを所定の復号鍵を用いて所定のプログラム

に復号し、復号した所定のプログラムをデータ処理部内の記憶手段に記憶させ、取り出し制限手段で復号手段で復号された所定のプログラム及び記憶手段に記憶された所定のプログラムの外部装置からの取り出しを制限することで、プログラムロード時における外部へのプログラムデータの漏洩を阻止することができるため、プログラムをロードする際に漏洩したプログラムデータを用いた違法行為を防止することが可能となる。

【０２７７】また、以上の説明からも明らかなように、本発明のプログラムロード方法は、復号ステップで、所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを所定の復号鍵を用いて所定のプログラムに復号し、復号した所定のプログラムをデータ処理部内の記憶手段に記憶させ、取り出し制限ステップで復号ステップで復号された所定のプログラム及び記憶手段に記憶された所定のプログラムの外部装置からの取り出しを制限することで、プログラムロード時における外部へのプログラムデータの漏洩を阻止することができるため、プログラムをロードする際に漏洩したプログラムデータを用いた違法行為を防止することが可能となる。

【０２７８】また、以上の説明からも明らかなように、本発明の記録媒体は、復号ステップで、所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを所定の復号鍵を用いて所定のプログラムに復号し、復号した所定のプログラムをデータ処理部内の記憶手段に記憶させ、取り出し制限ステップで復号ステップで復号された所定のプログラム及び記憶手段に記憶された所定のプログラムの外部装置からの取り出しを制限することを特徴とするプログラムを記録することで、プログラムロード時における外部へのプログラムデータの漏洩を阻止することができるため、プログラムをロードする際に漏洩したプログラムデータを用いた違法行為を防止することが可能となる。

【０２７９】また、以上の説明からも明らかなように、本発明の回路素子は、復号手段で、所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを所定の復号鍵を用いて所定のプログラムに復号し、復号した所定のプログラムを記憶手段に記憶させ、取り出し制限手段で復号手段で復号された所定のプログラム及び記憶手段に記憶された所定のプログラムの外部装置からの取り出しを制限することで、プログラムロード時における外部へのプログラムデータの漏洩を阻止することができるため、プログラムをロードする際に漏洩したプログラムデータを用いた違法行為を防止することが可能となる。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態として示すＤＶＤ－ＲＯＭドライブの構成を説明するためのブロック図である。

【図２】暗号化について説明するための図である。

55

【図３】本発明の実施の形態として示すＤＶＤ－ＲＯＭドライブにおいて、ファームウエアを更新する際の動作について説明するためのフローチャートである。

【図４】同ＤＶＤ－ＲＯＭドライブにおいて、アップデート関数によるファームウエア更新動作について説明するための第１のフローチャートである。

【図５】同ＤＶＤ－ＲＯＭドライブにおいて、アップデート関数によるファームウエア更新動作について説明するための第２のフローチャートである。

【図６】同ＤＶＤ－ＲＯＭドライブにおいて、ファームウエア更新処理後、更新が成功したかどうかを確認する動作について説明するためのフローチャートである。

【図７】同ＤＶＤ－ＲＯＭドライブのＣＰＵの別の構成を説明するためのブロック図である。

【図８】本発明の第２の実施の形態として示すＤＶＤ－ＲＯＭドライブの構成を説明するためのブロック図である。

【図９】同ＤＶＤ－ＲＯＭドライブの復号部の構成について説明するための図である。

【図１０】同ＤＶＤ－ＲＯＭドライブの暗号化部の構成について説明するための図である。

【図１１】同ＤＶＤ－ＲＯＭドライブにおいて、アップデート関数によるファームウエア更新動作について説明するための第１のフローチャートである。

【図１２】同ＤＶＤ－ＲＯＭドライブにおいて、アップデート関数によるファームウエア更新動作について説明するための第２のフローチャートである。

【図１３】同ＤＶＤ－ＲＯＭドライブにおいて、ファームウエア更新処理後、更新が成功したかどうかを確認する動作について説明するためのフローチャートである。

【図１４】本発明の第３の実施の形態として示すＤＶＤ－ＲＯＭドライブの構成を説明するためのブロック図である。

56

【図１５】同ＤＶＤ－ＲＯＭドライブの復号部の構成について説明するための図である。

【図１６】同ＤＶＤ－ＲＯＭドライブにおいて、マイクロプログラムをロードする際の動作について説明するためのフローチャートである。

【図１７】改竄防止のための検証プログラムが添付された暗号化プログラムが生成される際の動作について説明するためのフローチャートである。

【図１８】検証プログラムが添付された暗号化プログラムを実行するＤＶＤ－ＲＯＭドライブの動作について説明するためのフローチャートである。

【図１９】検証プログラムの動作を説明するためのフローチャートである。

【図２０】検証プログラム、検証データが添付されたプログラム本体を示した図である。

【図２１】ハッシュ関数について説明するための図である。

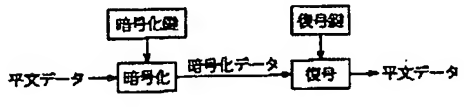
【図２２】検証プログラム、検証データが添付されたプログラム本体を暗号化した様子を示した図である。

【図２３】暗号化されたデータにＣｈｅｃｋ　Ｓｕｍデータを添附した様子を示した図である。

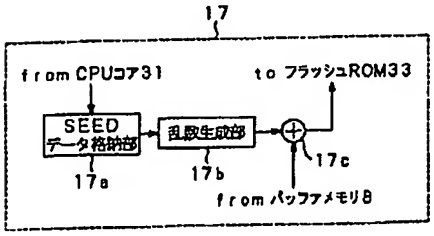
【符号の説明】

１　ＤＶＤ－ＲＯＭ（Digital Versatile Disc-Read Only Memory）、２　光学ピックアップユニット、３　スピンドルモータ、４　リードプロセッサ、５光学ピックアップユニットドライバ、６　スピンドルモータドライバ、７　ＤＶＤデコーダ、８　バッファメモリ、９　ＣＰＵ（Central Processing Unit）、２０　ＣＰＵコア、２１　ブートＲＯＭ（Read Only Memory）、２１ａ　暗号化処理部、２２　フラッシュＲＯＭ、２３　ＲＡＭ（Random Access Memory）、３１　外部バスコントローラ

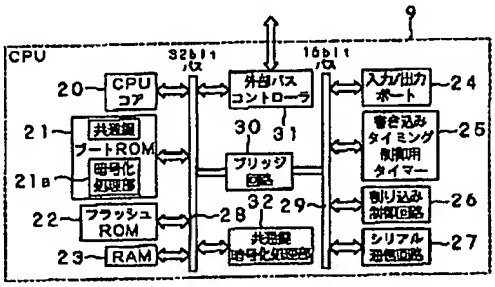
【図２】



【図９】

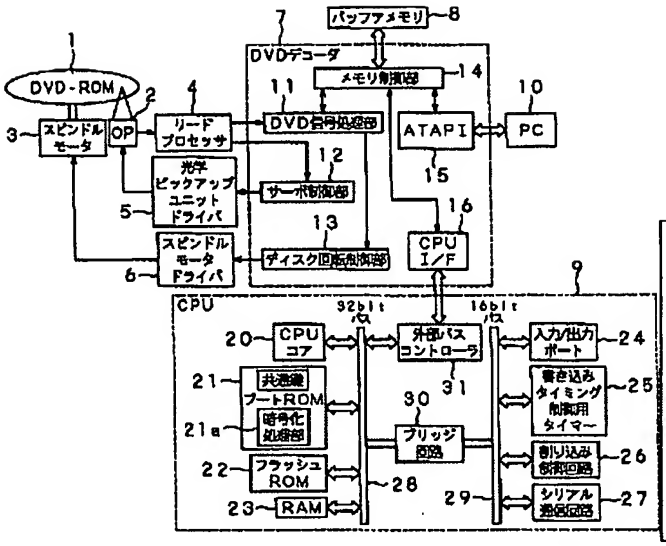


【図７】

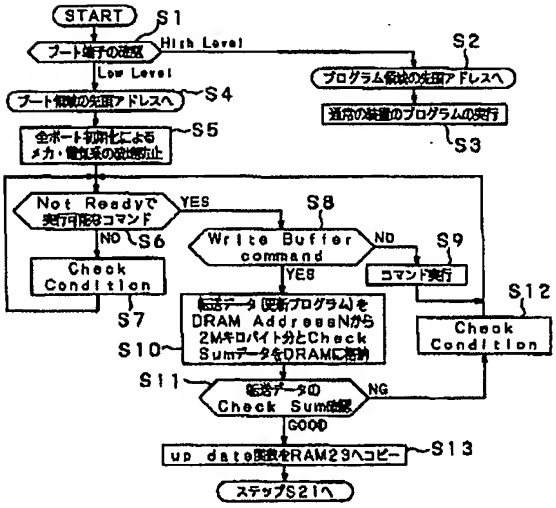


【図２０】

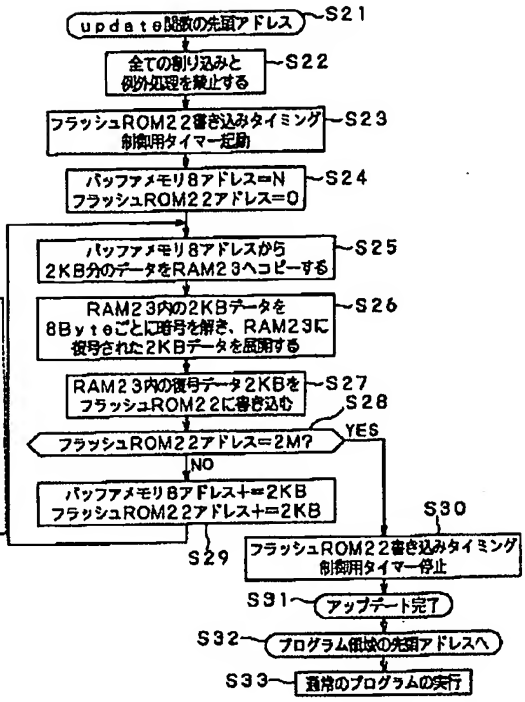
【図１】



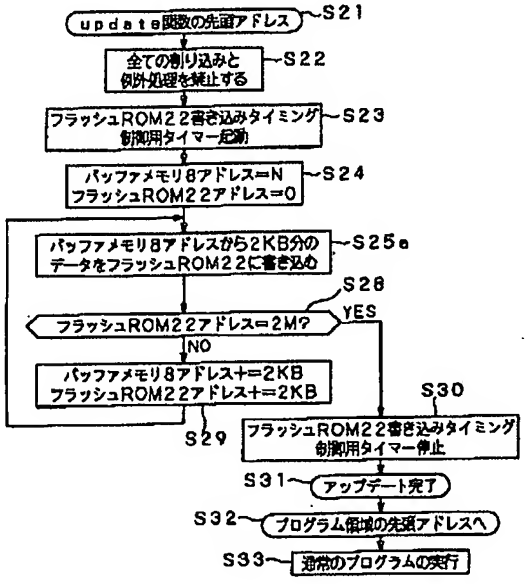
【図３】



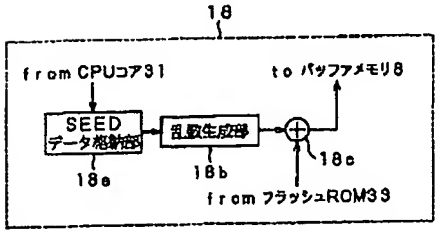
【図４】



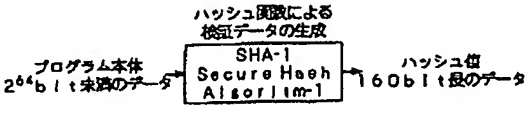
【図５】



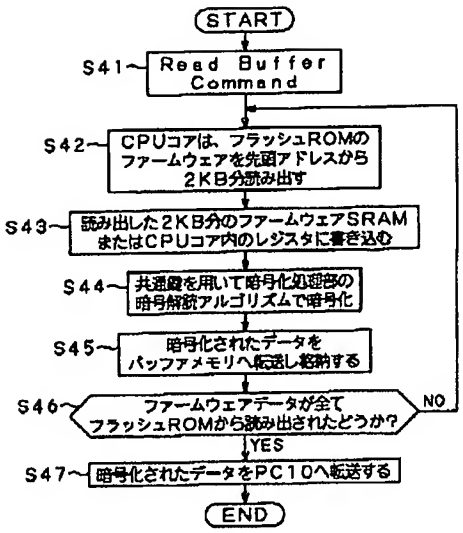
【図１０】



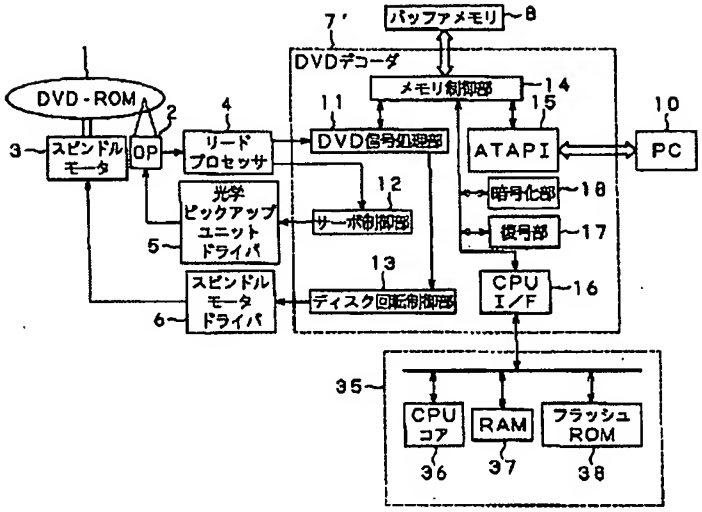
【図２１】



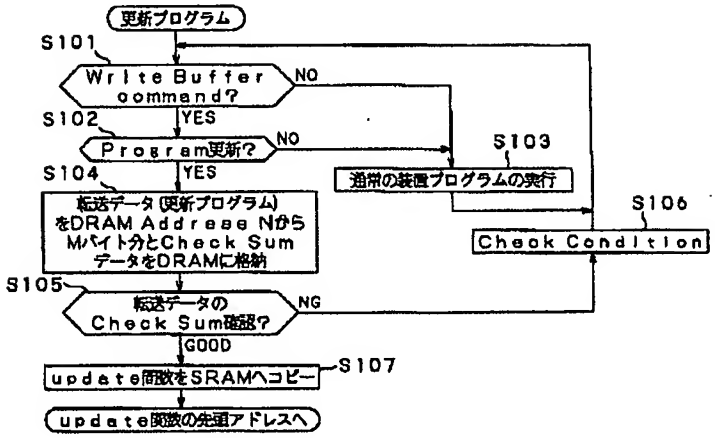
【図６】



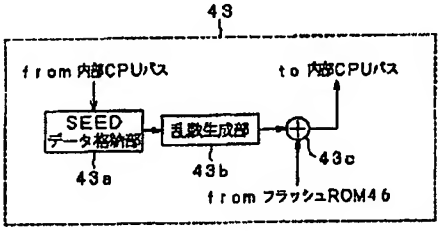
【図８】



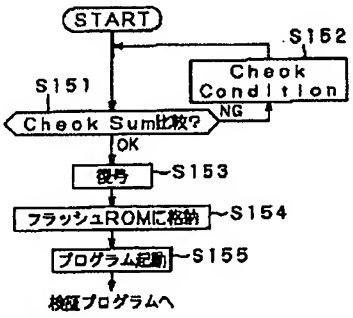
【図１１】



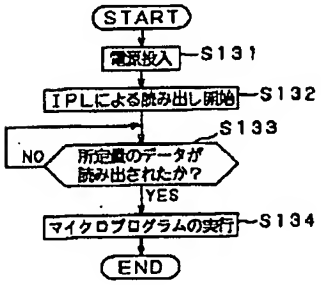
【図１５】



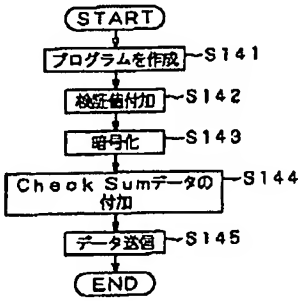
【図１８】



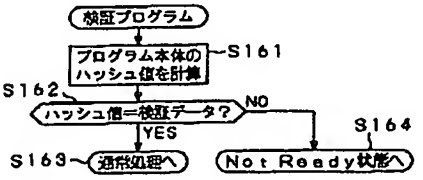
【図１６】



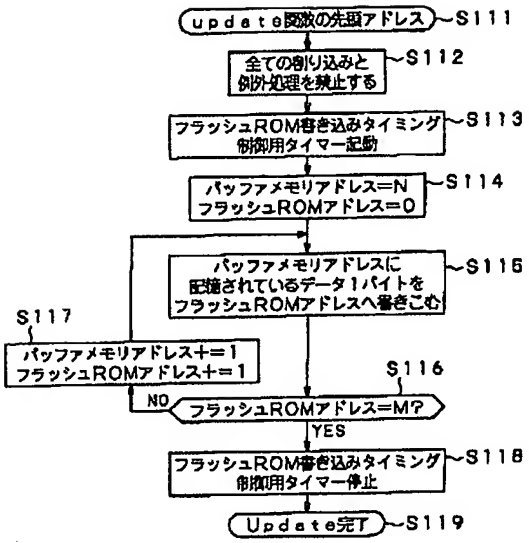
【図１７】



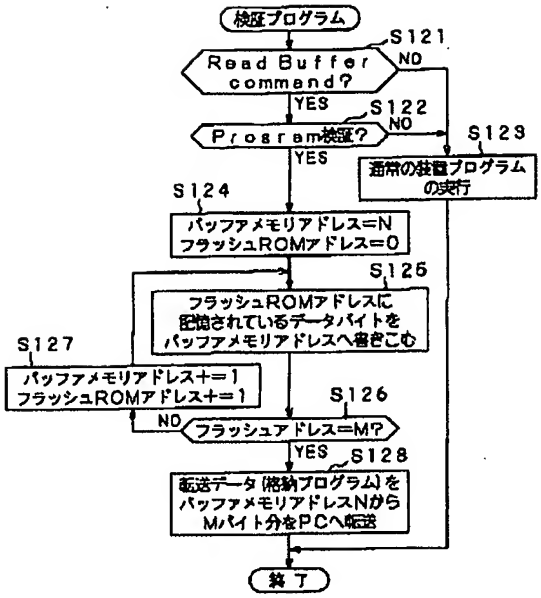
【図１９】



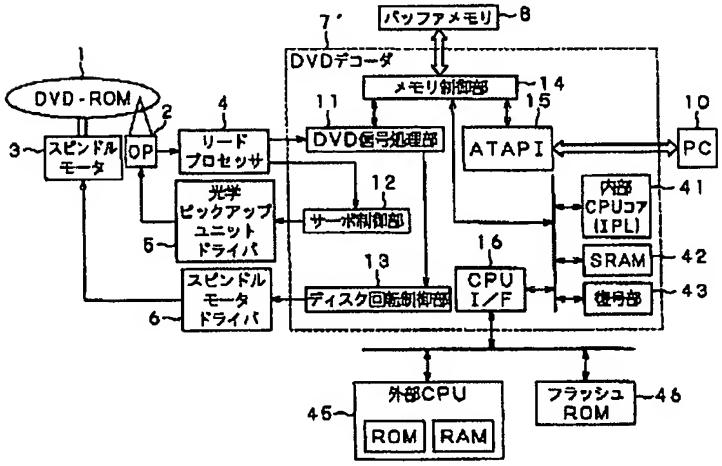
【図１２】



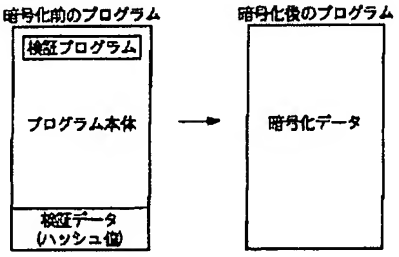
【図１３】



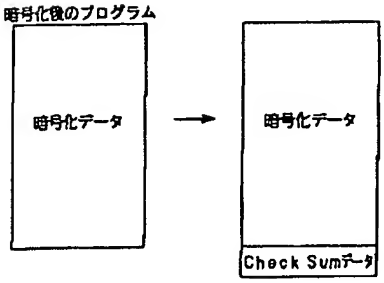
【図１４】



【図２２】



【図２３】



フロントページの続き

Ｆターム(参考) 5B017 AA08 CA15
5B076 FA00
5J104 EA18 NA02 NA12